AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 107–611

THE ROLE OF TECHNOLOGY IN PREVENTING THE ENTRY OF TERRORISTS INTO THE UNITED STATES

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

OCTOBER 12, 2001

Serial No. J–107–43

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

81–248 PDF WASHINGTON : 2002

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ORRIN G. HATCH, Utah
JOSEPH R. BIDEN, JR., Delaware	STROM THURMOND, South Carolina
HERBERT KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ARLEN SPECTER, Pennsylvania
RUSSELL D. FEINGOLD, Wisconsin	JON KYL, Arizona
CHARLES E. SCHUMER, New York	MIKE DEWINE, Ohio
RICHARD J. DURBIN, Illinois	JEFF SESSIONS, Alabama
MARIA CANTWELL, Washington	SAM BROWNBACK, Kansas
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

DIANNE FEINSTEIN, California, *Chairwoman*

JOSEPH R. BIDEN, JR., Delaware	JON KYL, Arizona
HERBERT KOHL, Wisconsin	MIKE DEWINE, Ohio
MARIA CANTWELL, Washington	JEFF SESSIONS, Alabama
	MITCH MCCONNELL, Kentucky

DAVID HANTMAN, *Majority Chief Counsel*
STEPHEN HIGGINS, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cantwell, Hon. Maria, a U.S. Senator from the State of Washington	41
DeWine, Hon. Mike, a U.S. Senator from the State of Ohio	11
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	1
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	6
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	105

WITNESSES

Camarota, Steven A., Director of Research, Center for Immigration Studies, Washington, D.C.	54
Collier, M. Paul, Executive Director, Biometrics Foundation, Gaithersburg, Maryland	89
Doonan, Tony, Vice President, Automated Fingerprint Identification Systems; accompanied by Greg Spadorcio, Director, Business Solutions, NEC Technologies, Inc., Gold River, California	74
Fine, Glenn A., Inspector General, Department of Justice, Washington, D.C.	13
Ryan, Mary A., Assistant Secretary for Consular Affairs, Department of State, Washington, D.C.	33
Ward, David, President, American Council on Education, Washington, D.C.	65
Ziglar, James W., Commissioner, Immmigration and Naturalization Service, Department of Justice, Washington, D.C.	24

SUBMISSIONS FOR THE RECORD

Goode, Ted, Director of Services for International Students and Scholars, University of California at Berkeley, Berkeley, California, statement	104
Immigration and Naturalization Service, Department of Justice, Washington, DC, visa information on terrorist hijackers of September 11, 2001, list	105
Oracle Corporation, Larry Ellison, Chairman and Chief Executive Officer, Redwood Shores, CA, letter	106

THE ROLE OF TECHNOLOGY IN PREVENTING THE ENTRY OF TERRORISTS INTO THE UNITED STATES

FRIDAY, OCTOBER 12, 2001

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

The subcommittee met, pursuant to notice, at 10:04 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein, chairman of the subcommittee, presiding.

Present: Senators Feinstein, Cantwell, Kyl, and DeWine.

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

Chairman FEINSTEIN. If I might, I would like to call this hearing to order.

There will be two panels. All written statements will be placed in the record. The ranking member is Senator Jon Kyl, who sits to my right. We will begin with opening statements and then proceed directly to the panels.

Today, the Subcommittee on Technology, Terrorism and Government Information is holding a hearing on the role of technology in preventing the entry of terrorists into the United States. We hold this hearing in the wake of the September 11 terrorist attacks on our Nation. These events have triggered concern about the shortcomings of the immigration and visa system of our country.

Just yesterday, the Department of Justice released information indicating that 13 of the 19 terrorist hijackers had entered the United States legally with valid visas. Of the 13, 3 of the hijackers had remained in the United States after their visas had expired. The INS had no information on six of the hijackers.

I would like to enter that information into the record.

Clearly, something is wrong with our system. The purpose of this hearing is to determine the extent to which gaps in our visa and admission system have frustrated efforts to identify and bring to justice the perpetrators of these attacks. More importantly, we would like to determine the extent to which these vulnerabilities will expose us to future attack.

Today, I see three areas of vulnerability in our immigration system: first, an unregulated visa waiver program in which 23 million people arrive in this country annually from 29 different countries with little scrutiny; second, an unmonitored non-immigrant visa

system in which 7.1 million tourists, business visitors, foreign students and temporary workers arrive. To date, the INS does not have a reliable tracking system to determine how many of these visitors left the country after their visas expired.

Third, among the 7.1 million non-immigrants, 500,000 foreign nationals entered on foreign student visas. The foreign student visa system is one of the most underregulated systems we have today.

I believe most foreign students legitimately come to the United States to study, and indeed they provide a great contribution, certainly a financial contribution as well as others, to our institutions. However, I do have a concern that in the last 10 years more than 16,000 students came from terrorist-supporting states such as Iran, Iraq, Sudan, Libya and Syria.

Let me give you an example of why this is a problem. In the early 1990s, officials at six colleges, three of which were in California, were convicted of taking bribes, providing counterfeit education documents, and fraudulently applying for foreign student visas so that more than 100 foreign nationals could gain easy entry to the United States. The officials from the six colleges were convicted. Some served time in prison, others paid monetary fines and restitution. It is unclear what steps INS took to find and deport the foreign nationals involved in the scheme.

There are other examples of the potential for gross misuse of the visa system. In 1991, the Washington Post reported that United Nations weapons inspectors in Iraq discovered documents detailing an Iraqi government strategy to send students to the United States and other countries to specifically study nuclear-related subjects to develop their own program. One of these students, Samir Al Araji, received his doctorate in nuclear engineering from Michigan State University. He then returned to Iraq to head its nuclear weapons program.

In 1998, the Richmond Times and New York Times did extensive reports on Rihab Taha, the mastermind of Saddam Hussein's germ warfare arsenal. Also known as "Dr. Germ," Taha studied in England on a student visa. England is one of the participating countries in the visa waiver program, which means if she could have gotten a fraudulent passport from England, she could have come and gone without a visa in the United States.

Now, why do I mention all of this? I think this sounds a wake-up call that there are many things in our system that are clearly broken. And this isn't a new problem. We have had plenty of warning of the weaknesses of our immigration system that helped lead to the September 11 attack. In fact, vulnerabilities in the system, for example, have been documented as far back as 1979, when during the Iranian hostage crisis the INS was unable to locate 9,000 of the estimated 50,000 Iranian students studying in the United States.

Now, this is a much bigger problem than just students because overall more than 30 million temporary visitors enter the United States, and that number doesn't take into account the 500 million entries at our land borders and ports of entry each year. These are people coming into the country, leaving the country, some of whom are United States nationals, many of whom are from other countries as well. Actually, two-thirds of these are non–U.S. citizens.

What these numbers show is that without an adequate tracking system, our country becomes a sieve, which it is today, creating ample opportunities for those who would do us harm to enter and to establish their operation without detection.

What I would like to get from this hearing is new solutions to the ongoing problems. One, the porous nature of our borders, along with INS' unreliable recordkeeping, have contributed to the agency's inability to keep out criminals and terrorists, and certainly their inability to track their whereabouts once they are here.

Secondly, in an era in which terrorists use satellite phones and encrypted e-mail, the INS, our Nation's gatekeeper, is considered by many observers to still be in the technological dark ages. The agency is still using paper files and archaic computer systems that are often non-functioning. They do not communicate with each other and they do not integrate well with other law enforcement systems.

Third, about 40 to 50 percent of the estimated 7 to 9 million illegal immigrant population are visa overstayers. These are people who enter the United States legally but violate the terms of their visas by staying beyond the permitted time.

Fourth, unlike most countries, the United States does not require exit visas—only a firm filled out by the visa-holder that is often not entered into an INS database for months, and in some cases a year later.

Fifth, the names of applicants are fed into a lookout system, a computerized database of some 5.7 million names fed and reviewed by the INS, U.S. Customs and the State Department. But this system is not failsafe. Because the lookout system used by American consular offices is based on a name check alone, it is vulnerable to evasion, not to mention document fraud and identity theft. An example of that is two of the alleged hijackers, Khalid Almidhar and Hawaf Alhazmi, made the watch list only after they gained entry to the United States.

And the watch list has not always helped. Sheik Omar Abdel–Rahman, the spiritual leader of the men involved in the 1993 World Trade Center bombing, legally entered the country on a visa, although he was already on a watch list of suspected terrorists. He was subsequently convicted in a conspiracy to blow up the New York World Trade Center.

Now, what is the conclusion? We are here to examine ways in which we can better utilize existing technologies to assist these agencies in preventing those who have the intent and who would carry out the goal of mass destruction from entering and staying in the United States.

In particular, I am interested in learning more about the feasibility of creating tamper-resistant visas and passports and establishing a non-immigrant tracking system using biometric data to verify the identity of persons seeking to enter the United States.

Along this line, yesterday I met with Larry Ellison, the CEO of Oracle. Senator Kyl did, as well. Mr. Ellison has offered—and I hope I will have a written statement from him and read that when I receive it at a point—well, I do have it. "Oracle takes seriously our responsibility in these difficult times. As we discussed, Oracle is prepared to provide, free of charge, the Oracle software licenses

for both testing and production of a complete national identification database."

Now, what he is saying is that they are prepared to devote some 1,500 engineers in a very timely way to put together the software of a database which could be entirely voluntary that would interrelate with other databases the United States has to form a national database.

One of the things that I think both Senator Kyl and I have discovered is that the credit industry of our country has the biggest database, and that the credit card is a much better identifier than anything we have nationally. Even a pilot's license today is just a scrap of paper that the pilot tears out of an overall piece of paper, very easily reproduced and certainly not at all fraud- or tamper-resistant.

So we would like to examine today how these new technologies could be used to establish an entry/exit system that could be integrated with the current lookout systems used by the INS, the State Department, and Federal law enforcement agencies.

Finally, we hope our panelists will offer concrete suggestions on the steps Congress should take to build the technological infrastructure of our Federal agencies so that they can better protect the United States ports of entry and our borders from future terrorist attack.

I would like particularly to commend my colleague on my right. Senator Kyl and I have worked closely on this subcommittee for a number of years, for the past 2 or 3 years under his chairmanship, and it has been a great pleasure for me. I think his leadership in this area has been important and significant, and we look forward to working together to craft bipartisan legislation that can come out of this committee to solve some of the problems I have just mentioned.

[The prepared statement of Senator Feinstein follows.]

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

INTRODUCTION

We hold this hearing in the wake of the September 11th terrorist attacks on the United States. Those horrific events have triggered concern about the shortcomings of the immigration and visa system.

Just yesterday, the Department of Justice released information indicating that 13 of the 19 terrorist hijackers had entered the U.S. legally with valid visas. Of the 13, three of the hijackers had remained in the U.S. after their visas had expired. The INS had no information on 6 of the hijackers.

Clearly, something tragically went wrong in our immigration system.

The purpose of this hearing is to determine the extent to which gaps in our visa and admissions systems have frustrated our efforts identify and bring to justice the perpetrators of the terrorist attacks. More importantly, we would like to determine the extent to which these vulnerabilities will expose us to future terrorist attacks.

Today, I see three areas of vulnerability in our immigration system:

(1) an unregulated visa waiver program, in which 23 million people arrived with little scrutiny in FY 2000 from 29 different countries.

(2) an unmonitored nonimmigrant visa system, in which 7.1 million tourists, business visitors, foreign students, and temporary workers arrived. To date, the INS does not have a reliable tracking system to determine how many of these visitors left the country after their visas expired.

(3) Among the 7.1 million nonimmigrants, 500,000 foreign nationals entered on foreign student visas. The foreign student visa system is one of the most under-regulated systems we have today.

I believe most foreign students legitimately come to the U.S. to study and, indeed, they provide a great contribution to our institutions of higher learning.

However, I do have a concern that in the last 10 years, more than 16,000 students came from such terrorist supporting states as Iran, Iraq, Sudan, Libya, and Syria. Let me give you an example of why this is a problem for me:

In the early 1990s, officials at six colleges, which of which were in California, were convicted of taking bribes, providing counterfeit education documents and fraudulently applying for foreign student visas so that more than 100 foreign nationals could gain easy entry in to the U.S.

The officials from the six colleges were convicted; some served time in jail, others paid monetary fines and restitution. It is unclear what steps the INS took to find and deport the foreign nationals involved in this scheme.

There are other examples of the potential for gross misuse of the foreign student visa.

In 1991, the Washington Post reported that the United Nations weapons inspectors in Iraq discovered documents detailing an Iraqi government strategy to send students to the United States and other countries to specifically study nuclear-related subjects to develop their own program. One of those students, Samir AI Araji (Sa-meer Al A- rah- hee), received his doctorate in nuclear engineering from Michigan State University and then returned to Iraq to head its nuclear weapons program.

In 1998, the Richmond Times and New York Times did extensive reports on Rihab Taha, the mastermind of Saddam Hussein's germ warfare arsenal. Also known as "Dr. Germ," Taha studied in England on a student visa.

England is one of the participating countries in the Visa Waiver program, which means if she could have gotten a fraudulent passport from England, she could have come and gone without a visa in the United States.

These instances should have provided a wake-up call that something in our system was clearly broken:

This is not a new problem. We have had plenty of warning of the serious weaknesses in our immigration system that led to the horrific September 11 attacks.

In fact, vulnerabilities in the Immigration and Naturalization Service's monitoring system, for example, have been documented as far back as 1979, when during the Iranian hostage crisis, the INS was unable to locate 9,000 of an estimated 50,000 Iranian students studying in the United States.

Overall, more than 30 million temporary visitors enter the U.S. each year. That number does not take into account the 500 million entries at our land borders and ports of entries each year. Two thirds of those entrants are non-U.S. citizens.

What these numbers show is that without an adequate tracking system, our country becomes a sieve, creating ample opportunities for terrorists to enter and establish their operations without detection.

What I'd like to get from this hearing is new solutions for the following ongoing problems:

(1) The porous nature of our borders along with the INS's unreliable record keeping, have contributed to the agency's inability to keep out criminals and terrorists-and to track their whereabouts once they are here.

(2) In an era in which terrorists use satellite phones and encrypted e-mail, the INS-our nation's gatekeeper-is considered by many observers to still be in the technological dark ages. The agency is still using paper files and archaic computer systems that are often non-functioning, do not communicate with each other, and do not integrate well with other law enforcement systems.

(3) About 40 to 50% of the estimated 7 to 9 million illegal immigrant population are visa overstayers-people who entered the U.S. legally, but later violated the terms of their visas by staying beyond the permitted period of time.

(4) Unlike most countries, the United States does not require exit visas-only a form filled out by the visa holder that is often not entered into an INS database for months and, in some cases, a year later.

(5) The names of applicants are fed into a "lookout" system, a computerized database of some 5.7 million names fed and reviewed by the INS, U.S. Customs and the State Department. This system is hardly failsafe.

Because the look-out system used by American consular offices is based on a name check, alone, it is vulnerable to evasion, not to mention document fraud and identity theft.

For example:

> Two of the alleged hijackers, Khalid Almihdhar and Hawaf Alhazmi, made the watch list only after they had gained entry into the United States. And the watch list has not always helped: Sheik Omar Abdel-Rahman, a spiritual leader of the men involved in the 1993 World Trade Center bombing,

legally entered the country on a visa, although he was already on the "watch list" of suspected terrorists. He was subsequently convicted in a conspiracy to blow up the World Trade Center.

CONCLUSION

We are here today to examine the ways in which existing technologies could assist these agencies in preventing those who are intent on carrying out the goal of mass destruction from entering and staying in the United States.

In particular, I would be interested to learn more about the feasibility of creating tamper-resistant visas and passports and establishing a nonimmigrant tracking system using biometric data to verify the identity of persons seeking to enter the U. S.

We will also examine how these new technologies could be used to establish an entry-exit system that could be integrated with the current look-out systems used by the INS, State Department and federal law enforcement agencies.

Finally, I will ask our panelist to offer concrete suggestions on the steps Congress should take to build the technological infrastructures of our federal agencies so that they may better protect the U.S. ports of entry and our borders from future terrorist attacks.

As we enter into these discussions today, it is important to recognize that increased technology, alone, is not a substitute for adequate number of personnel, adequate training for that personnel, and a cooperative relationship and spirit among the agencies charged with protecting our nation's borders, as well as our national security.

Today's hearing will examine the use of technology. Future hearings will examine some of the other important steps we can take to achieve these goals.

I look forward to hearing today's testimonies.

So, Senator Kyl, if you have some comments.

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

Senator KYL. Thank you very much, Senator Feinstein.

Much has been made of the unity that has existed since September 11, including here in Washington. As Senator Feinstein just said, that unity on this subcommittee existed from the very beginning, going back several years ago. We have jointly sponsored legislation, held hearings, made recommendations, and we will continue to do so.

I will tell you that there will not be one iota of difference between the position of the chairman of the subcommittee and my position. We will move together exactly together, and I think we will be able to ensure that our colleagues will be with us.

So a message to the administration and our witnesses here: we really appreciate your presence here, but we are going to be offering some ideas that haven't been implemented in the past by the administration, by any administration. And since all of you don't have to take credit or blame for positions of the past, don't; be willing to think openly about new ideas that may come from the Congress because we are going to be united in what we are recommending.

I agree with absolutely everything that the chairman just said and will just summarize some additional thoughts here.

Just as the bill that we passed last night is not the answer—I think Don Rumsfeld said there is no one silver bullet here in this war against terrorists, but there are a lot of individual pieces. Just like we see the FBI putting its case together meticulously, taking one little bit of data here and another bit of data there and connecting it all up and then finally they know what the threat is, we

too will put together a mosaic of things that will enable us to win this war.

The bill that we passed last night is one step. The proposals that Senator Feinstein has made here will be another important step. Do they solve everything? No, but they certainly deal with this immigration component.

Look at the headline in the Washington Post this morning: "INS Stumped on How Some Hijackers Entered the United States." No reflection on Mr. Ziglar. Obviously, he had nothing to do with the policies that bear on the deficiencies in INS at this moment, but obviously we are going to have to fix this problem.

Senator Feinstein alluded to the statistics, and one question I will ask you, Commissioner Ziglar, is do we know anything more about the actual status. I think on six of the people there is no record of any entry into the country, but I will get to that question later. In any event, obviously this cannot continue to be the case if we are going to ensure that bad elements are not permitted to be guests in the United States.

Senator Feinstein mentioned three specific things. The visa waiver program; we have clearly got to reform that. The unmonitored visa system generally, with no tracking, and so on, and the exit/entry component of that; we clearly have to fix that. The student visa program specifically; we clearly have to have more monitoring and reporting on that.

In addition to that, we have infrastructure needs, and I am sure this is music to some of your ears. You will tell us what they are and we hopefully will respond by providing you the resources that you need, both in terms of personnel—and by the way, this is personnel at the borders, at our immigration offices, our consular offices all around the world—we need more personnel as well as infrastructure.

We need to develop and use new technology that Senator Feinstein alluded to, including fraud-proof documents. This is an absolute must now. We are not talking about a national I.D. card, but we are talking about a method by which the United States can ensure that its laws are enforced with respect to the guests that we invite into the country. We are going to have to resolve conflicts that currently exist between information systems in the INS and the State Department.

Finally, let me just mention a few other quick questions and then I really want to hear from the witnesses. Here are some of the questions we are going to need to get some answers to.

Should INS replace its computer information system at all borders and put in the same system used by the State Department? How much would it cost? Should the State Department consider using facial recognition biometrics for all visa applicants? Should the INS consider using facial biometrics at points of entry? How about the role of fingerprint biometrics? What would the cost be to do that?

Should U.S. authorities receive background information on every visa-holder before he or she is allowed to exit an airport and enter the United States? I mentioned the exit/entry system. What is the status there, and how can we get that completed?

On foreign student visas, will the new system be maintained jointly by the State Department and INS? Will it have an automated linkage to the educational institutions? Will it require reporting and compliance, and how will this perhaps relate to the H–1B visa, the employment visa system? Regarding the waiver program, should we restrict participation to countries that only issue machine-readable passports?

Those are just a few of the questions that I think we need to deal with here.

Madam Chairman, I will ask that my full statement be put in the record. Let me just close with this comment. Last night, the President was asked a question at his news conference by one of the reporters. She said, well, you are asking us to support the Government's efforts here, but this is a war and I am just wondering when we are going to have to make some sacrifices in this war.

Let me add something to what the President said. I don't think it is much of a sacrifice for institutions that benefit from U.S. laws, like higher education—I hope there are some of you out here that are representing institutions of higher learning. You all benefit from these programs. The tuition you charge the foreign students really helps your coffers.

I was dismayed when the first reaction to Senator Feinstein's suggestion that maybe we needed to have a time-out here on these foreign student visas was, no, we can't do that; that will really hurt us financially. Well, what do you think has happened to the entire United States of America, our economy? Everybody was hurt dramatically by what happened and I don't think it is too much of a sacrifice to at least help us enforce the laws that you are benefitting from. Is that too much to ask?

We don't want to terminate these. We don't even, I suspect, at the end of the day, want to have a moratorium, but we are going to have an enforceable system. And you will have to help us or else there will have to be some kind of limitation. That is the way it is going to have to be throughout the rest of this country.

We are all living under a threat. My family is worried. My daughter is worried about her two little kids, and so on, and I will be darned if I am going to let them grow up and for decades, like we did during the Cold War, lead a life that is a life of fear, under constant threat, because they will never know what is going to hit them next.

We have got to win this war, and win it fairly quickly, and that means we have got to root out the base of terrorist support. That means we have got to protect our homeland. We all have to do that and it is not too much of a sacrifice for us to get together and figure out what kind of systems we can put together, not be turf-conscious.

It took us a long time to develop this INS system and so this has got to be the be-all and end-all. Maybe, maybe not. We have got to start thinking as a unified people to solve this problem because I don't want to live this way for the rest of my life and I don't want my kids and grandkids to.

So let's not think parochially here. Let's think about what we can do to band together and solve the problem. And I just want to say again there will not be one iota of difference between Senator Fein-

stein and me. I hope I haven't said anything here that she is going to disagree with now. But if so, then I agree with her, okay?

[Laughter.]

Senator KYL. We are going to work this through together, and we have got to work quickly. These reforms are not going to be easy or quick. They are going to cost some money, but we are going to have to do them as quickly as we can.

You yourselves answered the question that the President asked last night. What can we do? Well, every one of you now are thinking, okay, yes, there is something I can do to help here. Let's do it. Let's get together and do it and defeat this terrible scourge that is threatening us right now.

I really appreciate again all the witnesses who are here today. We will look forward to working with you.

[The prepared statement of Senator Kyl follows:]

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

Madam Chairwoman, thank you very much for holding this hearing today, one month and one day after the tragic events of September 11. I look forward to hearing the testimony of Inspector General Fine, Commissioner Ziglar, Ambassador Ryan, and the rest of the witnesses from the private sector—I am hopeful that all of these witnesses might shed some needed light on ways to fix our immigration and visa processing systems so that terrorists cannot enter or remain in the United States in violation of our laws.

The law enforcement and immigration enforcement provisions of the antiterrorism legislation that we are about to pass here in the Congress will provide many of the tools needed to weed out and stop terrorism.

Even with the passage of these provisions, however, the United States will continue to face overwhelming infrastructure and personnel needs at our consular offices abroad, along both our southern and northern border, and in our immigration offices throughout the United States. In conjunction with increasing personnel and infrastructure, the U.S. must, among other things, deprive terrorists of the ability to present altered international documents, and improve the dissemination of information about suspected terrorists to all appropriate agencies.

So legislative, and administrative, action in the coming months must go beyond the scope of the anti-terrorism package.

With regard to border and immigration personnel, it is encouraging that most everyone now agrees that a lot more personnel are needed. Over the past several years, many of us in Congress have worked hard to increase Border Patrol, Customs, and INS personnel. For the saddest of reasons, I hope the commitment to dedicate the funds for such personnel is finally there. All relevant agencies must also work hard to develop ways to effectively recruit and retain such personnel. Such efforts will be tracked by the Congress. With respect to State Department employees, significant increases in consular personnel must be made.

These personnel, whether they are inspectors, agents, or consular officers, must be equipped with the investigatory and security resources to weed out terrorists from ever getting into the country, and to stop them from staying here undetected, if they do get in. Finally, the many programs that we have, affecting immigration and the granting of visas, must be examined and changed, if they actually make abuse of the system by terrorists more possible.

Many questions need to be asked about the procedures in place on the ground. We must employ our technology better—or develop new technology—to catch alien terrorists:

- Should the INS replace its computer-information system at all borders and put in the same system used by the State Department? How much would it cost to do this? The current system is not equipped to accept all the information available from the State Department about a visa applicant or recipient.
- Should the State Department consider using facial recognition biometrics for all visa applicants, whether issued a visa or not, since the State Department requires a photograph for all visa applicants already? Should the INS consider using facial feature biometrics at its ports of entry? Are facial bio-

metrics superior to fingerprint biometrics? What would be the cost of implementing either a facial or fingerprint system?

• Should U.S. authorities receive background information on every visa holder before he or she is allowed to exit an airport and enter the United States?

• Where is the INS in its effort to develop the entry-exit system at airports and seaports? At land ports?

Many questions also need to be asked about nonimmigrant programs and the Visa Waiver Program. We should determine whether, without reform, such programs make it easier for terrorists to get here and stay here.

• Regarding foreign student visas, does the new INS-proposed student tracking system reflect concerns raised after the September 11 attack? Will the system overcome current deficiencies in processing and tracking? Will the new system be jointly maintained by the State Department and the INS? Will the new system have an automated linkage to educational institutions, so that they can inform INS when a student drops out or does not show up in the first place? Will a quarterly report be required of all educational institutions, including those that accept F, M, and J visas? Could other programs, such as the H1–B employment visa program, realistically be a part of such a system?

• Regarding the Visa Waiver Program, should we restrict participation to countries that issue only machine-readable passports? How can we be assured that the passport numbers of all Visa Waiver participants are entered into a database by the INS at ports of entry—even when the passport is not machine readable? Should the holders of non-machinereadable passports be required to go to "secondary" inspection at all ports?

Obviously, border, immigration, and visa-processing policies are very complex. To be sure of the utmost security, and also fairness to law-abiding immigrants, we are all going to have to work hard on these problems.

I am happy to report that a few things that we all knew needed to be done are included in the anti-terrorism package that will be passed and sent to the President soon. The legislation clarifies that the Federal Bureau of Investigation is authorized to share data from its "wanted lists," and any other information contained in its national crime-information system, with the State Department and the INS. This will help the INS and State Department identify suspected terrorists before they come to the United States, and, should they gain entry, will help track them down on our soil. It also allows the State Department, during a U.S. criminal investigation, to give foreign governments information on a case-by-case basis about the issuance or refusal to issue a U.S. visa. The anti-terrorism bill also will also clarify and toughen U.S. law prohibiting the entry of, and requiring the removal of, individual alien terrorists. In addition, the bill will give the Attorney General a newly designated, and reasonable, amount of time during which he may detain an alien believed to be inadmissible or deportable on terrorism grounds. Finally, the bill authorizes $36.8 million for quick implementation of the INS foreign student tracking system, a program I have long urged be reformed.

As ranking Member of the Judiciary Committee's Terrorism Subcommittee, I have long suggested, and strongly supported, many of the anti-terrorism and immigration initiatives now being advocated by Republicans and Democrats alike. In my sadness about the overwhelming and tragic events that took thousands of precious lives, I am resolved to push forward on all fronts to fight against terrorism. As I have outlined, changing our immigration and law- enforcement systems will be a complex undertaking, but it is absolutely necessary. Necessary, so that justice can be delivered to those who are responsible for the lives lost on September 11. And, so that the institutions of government can be reorganized in order that Americans can continue to live their lives in freedom.

Thank you, I look forward to hearing from all of our witnesses.

Chairman FEINSTEIN. Thanks very much.

Before I turn to Senator DeWine for an opening comment, I just want to respond. I think Senator Kyl and I and Senator DeWine and the other members will be on the same page.

The reason I initially proposed that we take that time-out to get our student visa program in shape was because it was very apparent to me, particularly after I reviewed the convictions that took place in San Diego, California, that we had a real problem there.

There was a resistance earlier on from schools to participate in providing the kind of information that was necessary.

The proposal for a 6-month time-out or moratorium or whatever you want to call it certainly got their attention. They have come in; there have been two meetings with my office. The school association will testify today. I believe they will testify that they want to be cooperative, that they are prepared to play a major role in providing the State Department, as well as INS, with the necessary information and to make bi-quarterly reports. So I think we have in the past two weeks made a great deal of progress in that regard.

Senator DeWine, do you have some comments you want to make?

STATEMENT OF HON. MIKE DEWINE, A U.S. SENATOR FROM THE STATE OF OHIO

Senator DEWINE. Very briefly, Madam Chairman, I have a full statement which I would ask permission to be part of the record.

Chairman FEINSTEIN. So ordered.

Senator DEWINE. Just briefly, let me thank you very much for holding this hearing. I thank our panelists for being here. We look forward to their testimony.

There are so many different aspects of the whole issue of terrorism and the whole issue of our borders, and let me just mention at the beginning one of the things that I have been thinking of.

In the Senate's anti-terrorism package that we were able to pass last night, I have asked the Attorney General, in consultation with appropriate agencies, to report back to us, to report back to the United States Congress, on how we as a country can use our national biometric systems, such as the Integrated Automated Fingerprint Identification System, more commonly known as the IAFIS system, which is maintained by the FBI, to better identify a person who holds a foreign passport or a visa when that person may be wanted in connection with a criminal or intelligence investigation in the United States or abroad before the issuance of a visa or their entry or exit from the United States.

Now, Madam Chairman, I recognize that INS technology is outdated and it is insufficient to meet these new demands. I believe that we should leverage the substantial investment taxpayers have made in the IAFIS system already to go ahead and expand that and to create a system of identification and verification that is fully integrated with all relevant Federal, State and local agencies, and to do that in real-time.

Currently, IAFIS has more than 48 million images, and exchanges information with almost all Federal, State and local law enforcement agencies. I am not saying that this system is perfect, but I am saying that we should use all of our available resources at our disposal. I think this is a tremendous resource and we need to build on that resource.

The days are long past when we have the luxury, if we ever did, of having different departments and different agencies in the Government using different systems. Those days are over and we have to build on the best system that we have, and I candidly believe that we have to look to the IAFIS system to build what we need to help all of us to keep our country more secure.

Madam Chairman, I thank you and I thank Senator Kyl and others who have expressed a real interest in this issue and I look forward to the testimony.

[The prepared statement of Senator DeWine follows:]

STATEMENT OF HON. MIKE DEWINE, A U.S. SENATOR FROM THE STATE OF OHIO

Madam Chairman, thank you for holding this important hearing on the "The Role of Technology in Preventing the Entry of Terrorists in the United States." I thank the witnesses for coming to testify today as well.

It seems to me that Congress has to make an important decision here—a decision about where to focus our resources. Today, every agency needs more resources to confront the challenges that Sept 11 has raised—INS and the State Department have the most pressing needs. The questions for these agencies is: Do we focus on trying to keep track of aliens we allow into the United States—or do we focus our resources on screening those who have asked permission to enter our country? The fact is that we have to walk and chew gum at the same time—we must do both. We must do a better job of screening aliens who enter the country, while at the same time keeping track of when and where those aliens enter and exit, and where they are while they are here.

Let me talk for a moment about the scope of the problem. Last year, the INS performed 529.6 million inspections of individuals who crossed our borders—by land, sea, and air. As noted in Commissioner Ziglar's written testimony, over a half billion personal contacts were made with INS inspectors at our ports-of-entry. After deducting American citizens who were inspected, 352 million aliens were inspected in 2000. A little less than a third of those aliens are permanent residents. That leaves 255 million inspections of temporary "non-immigrant" aliens who are crossing at U.S. ports-of-entry.

It appears that this is the pool of entries we are searching to find terrorists and others who are coming into the United States for illicit purposes. Out of 255 million inspections how on earth are our law enforcement and other agencies that are responsible for these individuals' entry supposed to identify 19 terrorists?

It's a vast challenge. But we expect it to be met. Congress expects you to be able to identify these people. Moreover, the American people expect the federal agencies who are responsible for these individuals to do it. Today we want to know how you plan to meet this challenge.

We know that it can be done—but it can only be done with technology. I would like to hear our panelists' ideas about how it can be done with technology. What is your plan for using all available technology to address this problem?

Let me tell you what I have been thinking. In the Senate's antiterrorism package, I have asked the Attorney general, in consultation with appropriate agencies, to report to Congress on how we can use our national biometric systems, such as the Integrated Automated Fingerprint Identification System (IAFIS) maintained by the FBI, to better identify a person who holds a foreign passport or a visa and may be wanted in connection with a criminal or intelligence investigation in the United States or abroad—before the issuance of a visa or their entry—or exit—from the United States.

I recognize that INS technology is outdated and insufficient to meet these new demands. We should leverage the substantial investment taxpayers have made-the IAFIS system to create a system of identification and verification that is fully integrated with all relevant federal, state, and local agencies—in real-time. Currently, IAFIS has more than 48 million images, and exchanges information with almost all federal, state, and local law enforcement agencies. I am not saying that this system is perfect, but I am saying that we should use all of our available resources at our disposal.

Again, thank you for participating today. I am looking forward to hearing the witnesses.

Chairman FEINSTEIN. Thanks very much, Senator DeWine.

One of the best sets of written testimony that I have seen in the time I have been in the Senate is the first person on the panel I am going to introduce, and that is the Inspector General of the United States Department of Justice, Mr. Glenn Fine. I would like to commend to everybody to read his full statement because it has got some very excellent specifics documenting where the systems fail today.

Mr. Fine is a Harvard Law graduate. He is a Rhodes Scholar. He has worked for the Inspector General's office since 1995. Before joining the Office of Inspector General, he was an attorney specializing in labor and employment law in Washington. From 1986 to 1989, he served as Assistant U.S. Attorney in Washington, D.C. He prosecuted more than 35 criminal jury trials, handled numerous grand jury investigations, and argued cases in the District of Columbia and the United States courts of appeals.

Mr. Fine, welcome to the committee.

STATEMENT OF GLENN A. FINE, INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. FINE. Thank you. Madam Chairwoman, Senator Kyl, Senator DeWine, members of the subcommittee, thank you for inviting me to appear before the subcommittee. My testimony this morning will focus on the work of the Office of the Inspector General that relates to the subject of technology and preventing the entry of terrorists into the United States.

Technology, particularly effective and reliable information technology systems, is a critical component in this effort, and nowhere are we more in need of effective IT systems than in the INS. Yet, the OIG's extensive work in the INS has revealed significant problems with that agency's development and implementation of its IT systems.

Two OIG audit reports concluded that the INS could not sufficiently track the status of its IT projects to determine whether progress was acceptable, given the amount of time and funds spent. We found that estimated completion dates for projects were delayed without explanation, costs continued to spiral upward with no justification for how funds were spent, and projects neared completion with no assurance for meeting performance and functional requirements. General Accounting Office reviews reached related conclusions about the INS IT systems.

These problems in managing and implementing technology systems affect the ability of the INS to fulfill its critical mission. Let me provide the subcommittee with one example of a specific INS system that I discuss in my written statement.

The INS' automated biometric identification system, known as IDENT, is used in part to identify individuals whom the INS apprehends or comes in contact with. It is an important system that scans two fingerprints and a photograph of an alien and compares them against records in the IDENT lookout and recidivist databases.

The INS envisioned that most of its operations, including the Border Patrol, investigations, detention and deportation, intelligence and inspections, would benefit from IDENT through its quick and accurate identification of individuals. However, an OIG inspection raised concerns about the quality of data placed in IDENT and INS training of its employees on the system. In a later review, the OIG again found problems with IDENT under tragic circumstances.

Rafael Resendez–Ramirez was a Mexican national accused of committing several murders in the United States. When local police searching for Resendez contacted INS investigators in Houston,

none of the INS investigators placed a lookout for him in IDENT. Consequently, when Border Patrol agents apprehended Resendez as he attempted to illegally cross the border into New Mexico, nothing in IDENT alerted them to the fact that he was wanted for murder or had an extensive criminal record. The Border Patrol therefore followed its standard policy and voluntarily returned him to Mexico. Resendez returned to the United States within days of his release and murdered several more people before surrendering.

A review of the Resendez case showed problems that were indicative of, and partly caused by, larger failings in the design and implementation of this information technology system. We found that training on IDENT for INS employees, particularly outside the Border Patrol, was ineffective or nonexistent. INS program offices, such as Investigations and Intelligence, viewed IDENT as a Border Patrol initiative and were not educated on how it could be useful to its mission. Also, IDENT was not, and still is not linked with the FBI's Integrated Automated Fingerprint Identification System, which Senator DeWine discussed, and the FBI's National Crime Information Center 2000 system.

The Resendez case vividly illustrated the need for sharing of information among Government agencies, and it spurred the FBI and the INS to begin to develop an integration plan. That plan is still under development.

In another OIG review, we assessed the INS' efforts to reduce the risks of the visa waiver program. This program permits citizens from 29 countries to enter the United States as visitors without first obtaining visas or being screened in any way prior to their arrival.

INS inspectors have, on average, less than one minute to check and decide on each applicant. Our review found that INS inspectors did not check all passports of visa waiver applicants against the INS computerized lookout system. We also noted that terrorists, criminals and alien smugglers have attempted to gain entry into the United States through the visa waiver program.

INS inspectors told the OIG that terrorists and criminals believed they would receive less scrutiny during the inspection process if they applied under the program. INS officials also told the OIG that the theft of passports from visa waiver countries was a serious problem. We tested a sample of stolen passports and found that almost 10 percent may have been used to successfully enter the United States. In addition, we found that 53 percent of the stolen passports in our sample had no lookout record in the INS system. We recommended that the INS take steps to systemically collect information about stolen passports and enter them into the lookout system.

Another OIG review examined the INS' tracking and identification of non-immigrant visa overstays. As Senator Feinstein discussed, these are visitors who enter the United States legally but fail to depart when required. The INS estimates that 40 to 50 percent of the approximately 7 million or more illegal aliens in the United States fit into this category.

Our review found that the principal INS system for tracking visa overstays, the Non–Immigrant Information System, was not producing reliable data either in the aggregate or on individuals. We

also found that the INS had no specific enforcement program to identify, locate, apprehend and remove overstays, and that using the INS data was of little use for locating them.

Also related to the issue of non-immigrant visa overstays, the OIG recently examined INS efforts to meet congressional directives to develop an automated entry and exit control system that would collect a record for aliens arriving in the United States from an I–94 card and automatically match these with I–94 departure cards. The OIG found that the INS has not properly managed the project. Despite having spent $31 million on the system, the INS was operating it at only a few airports and does not have clear evidence that it would meet its intended goals.

Other OIG reviews discussed in my written statement discuss problems in the FBI's information technology systems and the specific case of how two men entered and remained in the United States before being arrested on charges of attempting to bomb the Brooklyn subway system.

Technology alone, however, is not sufficient to prevent the entry of terrorists into the United States. In February 2000, the OIG issued a report that systematically examined the Border Patrol's efforts to control illegal activity along the northern border. We found that nearly 4,000 miles of border between the United States and Canada were woefully understaffed.

The Border Patrol realized this risk but, because of the low numbers of agents assigned to northern Border Patrol sectors, could not cover all shifts 24 hours a day, 7 days a week. Most Border Patrol officials we interviewed believe that around-the-clock coverage was the minimum acceptable level of coverage for northern Border Patrol stations. Force multipliers such as cameras, sensors and other technology can aid the Border Patrol in its surveillance and interdiction activities, but northern border sectors do not have adequate amounts of this equipment.

In sum, the effective implementation and management of technology is critical to helping prevent terrorists from entering this country. Among other recommendations cited in my written statement, we urge the INS and the FBI to ensure that their databases share information both with each other and with other Government agencies. It is also abundantly clear that more resources need to be devoted to the northern border. Technology can help in this effort, but there are too few agents and inspectors along this border.

We recognize that the issues involved in this problem are complex with no easy solutions and that the task is enormous. Solutions require strategic vision, strong leadership, individual and organizational accountability, and sustained follow-through. Implementation of effective technology needs to be a top priority of the INS, the FBI and other Government agencies because it is essential to protecting the integrity of the immigration system and the national security.

That concludes my prepared statement and I would be pleased to answer any questions.

[The prepared statement of Mr. Fine follows:]

STATEMENT OF GLENN A. FINE, INSPECTOR GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Madame Chairwoman, Senator Kyl, and Members of the Subcommittee on Technology, Terrorism, and Government Information:

I. INTRODUCTION

I appreciate the opportunity to appear before the Subcommittee on Technology, Terrorism, and Government Information to discuss the role of technology in preventing the entry of terrorists into the United States. My testimony this morning will focus primarily on programs and related technologies in the Immigration and Naturalization Service (INS), including problems in INS information technology systems, the Visa Waiver Program, controlling the northern border, and the potential for immigration document fraud. I also will address briefly information technology systems in the Federal Bureau of Investigation (FBI).

Conducting comprehensive oversight of INS programs, including reviews relating to information technology, has been a longstanding priority for the Office of the Inspector General (OIG). We have expended such effort in response to concerns expressed within the Department of Justice (Department) and Congress, as well as our own assessment, about how the INS was handling its important and diverse responsibilities. As the INS's budget and workforce have increased to more than $5 billion and 33,000 staff, the need for concerted OIG oversight similarly has increased.

At the outset of my remarks, I want to stress that while the OIG has noted serious deficiencies in INS operations and systems over the years, this should in no way diminish the important contributions thousands of INS employees make on a daily basis. These employees perform diligently, under very difficult circumstances, and their mission is critical to the proper functioning of our government.

Yet, as this statement will discuss, our reviews of INS programs and their associated information technology systems have revealed significant problems that leave gaps in the INS's attempts to secure the nation's borders. Over the past decade, the OIG has found serious process and management deficiencies in the INS. Many OIG reviews of INS programs have questioned the reliability of the agency 's automated information systems and the accuracy of the data produced by those systems. We see separate automated systems planned for almost every function in the INS, but many of these systems do not "talk" to each other and therefore cannot be used to meet other important agency missions. Furthermore, given the INS's track record in acquiring and managing information technology systems, the OIG is concerned that the INS will not have the managerial expertise or ability to bring all of its automation initiatives successfully to completion, particularly in a timely and cost-effective fashion.

I turn now to OIG reviews that relate to information technology problems and immigration issues that affect the INS's ability to prevent terrorists from entering the country.

II. OIG REVIEWS

A. INS MANAGEMENT OF INFORMATION TECHNOLOGY SYSTEMS

According to Department of Justice estimates, the INS has spent more than $290 million on automated systems in fiscal year (FY) 2001 and more than $260 million in FY 2000. All told, through fiscal year 2001, the INS planned to spend approximately $2.6 billion on its automation programs. However, two OIG reviews of the INS's management of its automation initiatives found lengthy delays in completing many automation programs, unnecessary cost increases, and a significant risk that finished projects would fail to meet the agency's needs.

A March 1998 OIG audit found that the INS did not adequately monitor its automation programs. We concluded that the INS lacked comprehensive performance measures and insufficiently tracked the status of its projects. Consequently, the INS could not determine if progress towards the completion of the projects was acceptable. As a result, we stated that the INS faced risks that: (1) completed projects would not meet the overall goals of the automation programs; (2) completion of the automated projects would be significantly delayed; and (3) unnecessary cost increases would occur.

In July 1999, the OIG issued a follow-up report which again found that the INS was not adequately managing its automation programs. In the 1999 audit, we noted that the INS still could not sufficiently track the status of its automation projects to determine whether progress was acceptable given the amount of time and funds

already spent. We reported that: (1) estimated completion dates for projects were delayed without explanation; (2) costs continued to spiral upward with no justification for how funds were spent; and (3) projects neared completion with no assurance for meeting performance and functional requirements.

We identified three causes for these problems. First, INS managers did not have a common base line of automation projects by which to focus their collective efforts. In fact, the INS had substantial difficulty providing us with a complete list of their automation projects. Second, project information needed for effective management and decision-making was not readily available. Third, INS managers did not develop, document, or implement basic management control processes necessary to ensure that projects would be completed on schedule and meet performance and functional requirements. The ultimate cost for the INS's automation programs was uncertain because actual costs incurred were unreliable and projected cost estimates were unsupported.

Furthermore, we found that the INS had not implemented adequate safeguards to ensure the accuracy of existing data that would be used by systems being developed or re-engineered, or the adequacy of future data inputs. As a result, new or existing INS systems could contain inaccurate or unreliable data.

Since these audits, the General Accounting Office (GAO) issued reports in August 2000 and December 2000 that reached related conclusions about the INS's management of its information technology programs. Those reports concluded that the INS does not have an enterprise architecture to ensure that the hundreds of millions of dollars it spends each year on new and existing technology will optimally support the INS's mission. The GAO also concluded that the INS did not have adequate processes in place to effectively manage its planned and ongoing information technology programs.

B. THE VISA WAIVER PROGRAM

The Immigration Reform and Control Act of 1986 created the Visa Waiver Pilot Program (VWPP), which permitted citizens from certain countries to enter the United States as visitors without first obtaining visas. The law allowed VWPP visitors to stay in the United States for up to 90 days per visit and required them to possess a round trip ticket and waive their rights to appeal immigration officers' determinations of admissibility or contest any deportation actions.

In October 2000, the program became permanent and is now known as the Visa Waiver Program. Currently, visa requirements are waived for citizens of 29 countries who wish to visit the United States.

In 1999, the OIG assessed the INS's efforts to minimize illegal immigration and security threats posed by abuse of the VWPP. Because visitors traveling for business or pleasure under the VWPP were not required to obtain visas, they were not screened in any way prior to their arrival at U.S. ports of entry. Instead, VWPP visitors presented their passports to INS inspectors on arrival. The inspectors observed the applicants, examined their passports, and conducted checks against a computerized lookout system to decide whether to allow applicants entry into the United States. This review by INS inspectors was the principal means of preventing illegal entry. INS inspectors had, on average, less than one minute to check and decide on each applicant.

As a result of our review, we found that INS inspectors did not query all VWPP passport numbers against the INS's computerized lookout system. In addition, our inspection noted that terrorists, criminals, and alien smugglers have attempted to gain entry into the United States through the VWPP.

INS inspectors told the OIG that terrorists and criminals believed they would receive less scrutiny during the inspection process if they applied under the VWPP and consequently would have a greater chance of entering the United States without being intercepted. In addition, several of these terrorists and criminals had criminal records that would have prevented them from obtaining a visa if they were required to apply for one. For the Subcommittee's information, I provide several examples of terrorists and criminals who have attempted entry into this country under the VWPP.

- One of the conspirators in the 1993 World Trade Center bombing entered the country on a photo-substituted Swedish passport in September 1992. When the terrorist arrived at John F. Kennedy International Airport in New York City, an INS inspector suspected that his passport had been altered. A search of his luggage revealed instructional materials for making bombs. The subject was detained and sentenced to six months' imprisonment for passport fraud. In March 1994, he was convicted for his role in the Trade Center bombing and sentenced to 240 years in prison.

• Two Irish VWPP applicants attempted to pass through an INS overseas pre-inspection facility in August 1998. INS inspectors questioned both applicants, one of whom admitted that he had served jail time for possession of explosives and had been a member of the Irish Republican Army (IRA). Irish immigration authorities informed the INS inspectors that this applicant was a current member of the Real IRA—a terrorist group that had broken away from the original IRA. INS inspectors felt that there was sufficient evidence to deny entry and both applicants were refused admission to the United States.

• In July 1988, the United Kingdom (U.K.) became the first country to join the VWPP. Seventeen months later, the INS's New York District Office reported a trend in which Nigerian drug couriers were using photo-substituted U.K. passports to facilitate their drug-smuggling activities. An INS intelligence report documented the apprehension of four Nigerian drug couriers within a four-day period by U.S. Customs officials. Two of the applicants presented photo-substituted passports. The INS report stated that "[t]he travel document of choice is an altered British passport."

During our review, the INS informed the OIG that the theft of passports from VWPP countries was a serious problem. Because these stolen passports are genuine documents, their fraudulent use is difficult for INS inspectors to detect. During our review, we tested a sample of 1,067 passports stolen from VWPP countries and found that almost 10 percent may have been used to successfully enter the United States. We also identified problems with the way the INS maintains its lookout system, including its failure to enter information about stolen VWPP passports into the lookout database in a timely or accurate manner. As a result, 567 stolen passports in our sample of 1,067 (53 percent) had no lookout record in the INS system. Of the 500 passport numbers that had lookout records, 112 (22 percent) were not entered accurately. This missing or inaccurate information reduced the effectiveness of the lookout system and increased the possibility that inadmissible VWPP applicants could enter the United States.

C. BORDER PATROL EFFORTS ALONG THE NORTHERN BORDER

In February 2000, the OIG issued a report that systematically examined the Border Patrol's efforts to control illegal activity along the northern border, reviewed how the Border Patrol collects and assesses information about illegal activity and responds to it, and evaluated the allocation of Border Patrol resources to the northern border.

The nearly 4,000 miles of border between the United States and Canada are managed by 8 of the Border Patrol's 21 sectors. As of September 30, 1999, 311 of the national total of 8,364 Border Patrol agents (3.7 percent) were assigned to northern border sectors. In keeping with the INS's strategic plan, the Border Patrol deployed 7,706 Border Patrol agents (92.1 percent of the total) to its nine southwest Border Patrol sectors. The remaining 347 agents were assigned to the coastal sectors, headquarters, INS regional offices, and the Border Patrol Academy. Currently, according to the INS, there are 334 Border Patrol agents assigned to the northern border.

Border Patrol sectors on the Canadian border face significant challenges, even though the volume of known illegal alien entries is much less than along the Mexican border. The OIG review reported an increase in illegal activity along the northern border, including an increase in alien and drug smuggling. But the INS was unable to assess the level of illegal activity along the northern border, given the limited personnel and equipment resources allotted to its eight northern Border Patrol sectors. However, it is clear that the level of illegal activity exceeds the Border Patrol's capacity to respond. We also found that other factors, such as the detailing of agents from the northern to the southwest border and lack of detention space to house apprehended aliens, further diluted the Border Patrol's enforcement capabilities along the northern border.

We concluded that the number of agents assigned could not adequately patrol the entire length of the northern border. Shifts with no Border Patrol coverage left the northern border open. INS Intelligence officers also told us that criminals monitor the Border Patrol's radio communications and observe their actions. The criminals know the times when the fewest agents are on duty and plan their illegal operations accordingly. The Border Patrol realized this risk but, because of the low numbers of agents assigned to northern border sectors, it could not cover all shifts 24 hours a day, 7 days a week. Most Border Patrol officials we interviewed believed around-the-clock coverage was the minimum acceptable level of coverage for northern Border Patrol stations.

"Force-multipliers" such as cameras, sensors, and other technology aid the Border Patrol in its surveillance and interdiction activities, but we found that northern border sectors do not have adequate amounts of this equipment. For example, at the time of our inspection, one northern border sector had identified 65 smuggling corridors along the more than 300 miles of border within its area of responsibility, but the sector had only 36 sensors with which to monitor these corridors.

The Border Patrol's Strategic Plan, issued in 1994, does not address the northern border until the plan's fourth and final phase. Phase I of the Strategic Plan was designed to control the San Diego and El Paso Corridors; Phase II to control South Texas and Tucson corridors; Phase III to control the remainder of the southwest border; and Phase IV to control the rest of the borders, including the northern border. At the time of our inspection in 2000, the Border Patrol was in Phase II of its strategic plan, and no date had been set for implementation of Phase IV. In addition, the strategic plan did not articulate the strategies that the Border Patrol would eventually use to control the northern border once it has achieved control of the southwest border.

The OIG recommended that the INS Commissioner outline the approach the Border Patrol would take to secure the northern border, including determining the minimum number of Border Patrol agents required to address existing gaps in coverage, determining the amount of intelligence resources needed to more accurately assess the level of illegal activity, and identifying and implementing accurate data collection methods to support decisions about personnel and equipment. INS eventually wrote a strategic plan regarding the northern border, but we understand that it has not been implemented. We also recommended that the Commissioner evaluate whether there was a continuing need to detail Border Patrol agents out of northern sectors.

D. NONIMMIGRANT OVERSTAYS

The INS estimates the number of illegal aliens in the United States at 5 million to 6 million, while others estimate the number to be even higher. A common perception about illegal aliens is that the vast majority enter the United States by surreptitiously crossing our land borders, primarily from Mexico. In fact, the INS estimates that approximately 40 to 50 percent of the illegal alien population entered the United States legally as temporary visitors but simply failed to depart when required. The INS refers to these illegal aliens as nonimmigrant "overstays." More than 90 percent of overstays are tourists or business visitors, but overstays also include students and temporary workers.

In a 1997 inspection, the OIG found that the principal INS record-keeping system for tracking nonimmigrant overstays, the Nonimmigrant Information System (NIIS), does not produce reliable data, either in the aggregate or on individual nonimmigrants. Normally, passengers arriving in the United States fill out an I–94 form and present it to the INS inspector upon arrival. The inspector collects the arrival portion of the form and returns the departure portion to the passenger. The arrival portion is sent to an INS contractor, who inputs the data into NIIS. When the person leaves the United States, the airlines are supposed to collect the departure portion of the I–94 form and provide it to the INS for input into NIIS. The data is then matched by NIIS to identify nonimmigrant overstays.

We found that the NIIS data is incomplete and unreliable due to missing departure records and errors in processing of the records. NIIS does not contain departure records for a large number of aliens, most of whom the INS assumes have left the United States. The INS believes that unrecorded departures result from airlines failing to collect departure forms, from aliens departing through land borders, from data entry errors, from records being lost through electronic transmission or tape-loading problems, or from the failure of the system to match arrival and departure records.

We also found that the INS had no specific enforcement program to identify, locate, apprehend, and remove nonimmigrant overstays, and we concluded that NIIS data would be of little use for locating aliens.

E. THE INS'S AUTOMATED I–94 SYSTEM

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 directed the Attorney General to develop an automated entry and exit control system that would collect a record for every alien departing the United States and automatically match these departure records with the record of the alien's arrival. This proposal was designed to replace the manual system of collecting I–94 cards and enable the INS, through on-line searching procedures, to identify lawfully admitted nonimmigrants who remain in the United Sates beyond the period authorized. In

2000, however, Congress extended the deadline for implementing the system for airports and sea border ports of entry until December 31, 2003, and for high-traffic land border ports of entry until December 31, 2004.

In response to this congressional requirement, the INS introduced a pilot system in 1997 to automate the processing of air passenger I–94 forms. This automated I–94 system captures arrival and departure data electronically and uploads non-U.S. citizen data to the INS's NIIS.

This summer, the OIG completed an audit of the design and implementation of the automated I–94 system and found that the INS has not properly managed the project. Despite having spent $31.2 million on the system from FY 1996 to FY 2000, the INS: (1) does not have clear evidence that the system meets its intended goals; (2) has won the cooperation of only two airlines; (3) is operating the system at only a few airports; and (4) is in the process of modifying the system. INS officials estimated that an additional $57 million would be needed for FY 2001 through FY 2005 to complete the system. These projections include development, equipment, and operation and maintenance costs.

As a result of our concerns, we made a series of recommendations to help ensure that the INS rigorously analyzes the costs, benefits, risks, and performance measures of the automated I–94 System before proceeding with further expenditures.

F. AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT)

In 1989, the INS began to develop an automated biometric identification system to identify quickly individuals who are apprehended or have come into contact with the INS. Biometrics are biological measurements unique to each person, such as fingerprints, hand geometry, facial patterns, retinal patterns, or other characteristics, that are used to identify individuals. Fingerprints are the most common biometric used by law enforcement agencies. Historically, without a biometric system, the INS had to rely upon the names provided by aliens who were apprehended when checking against their databases or other records. But aliens often used false names or different names during different apprehensions. Also, many persons have similar names, and spelling errors can result in problems identifying individuals accurately.

After several studies, in 1994 the INS began implementing the Automatic Biometric Identification System, called IDENT. IDENT was first deployed in the San Diego Border Patrol Sector and subsequently throughout the southwest border. IDENT workstations consist of a personal computer, camera, and a single-fingerprint scanner. During enrollment of individuals into IDENT, INS agents scan an individual's two fingerprints, take the individual's photograph, and enter basic apprehension information about the individual into the automated system. When this information is saved, IDENT matches the fingerprints of the individual against the corresponding fingerprints of all individuals in two central IDENT databases, the lookout database and the recidivist database.

In the 1996 Illegal Immigration Reform and Immigrant Responsibility Act, Congress directed the INS to expand the use of IDENT to "apply to illegal or criminal aliens apprehended Nationwide." INS officials envisioned that most of the agency's programs and operations—including the Border Patrol, Investigations, Detention and Deportation, Intelligence, Inspections, Benefits Adjudication, and the INS Service Centers—would benefit from the IDENT system through its quick identification of individuals and its ability to obtain information about them from previous encounters with the INS, including any criminal history.

In 1998, the OIG evaluated the INS's implementation of IDENT and found that the INS was enrolling less than two-thirds of the aliens apprehended along the U.S.-Mexico border into the IDENT system. In addition, the INS was entering the fingerprints in the IDENT lookout database of only 41 percent of the aliens deported and excluded in FY 1996; of these, only 24 percent had accompanying photographs even though the INS relies on photographs to confirm identification. We found virtually no controls in place to ensure the quality of data entered into the IDENT lookout database. As a result, we found duplicate records and invalid data. We also raised concerns that the INS had not provided sufficient training to its employees on the use of IDENT. These failures hampered the INS's ability to make consistent and effective use of IDENT.

G. THE RAFAEL RESENDEZ-RAMIREZ CASE AND THE OPERATION OF IDENT

In March 2000, the OIG issued another review that implicated the IDENT system in tragic circumstances. The OIG examined how the INS handled its encounters with Rafael Resendez-Ramirez (Resendez), a Mexican national accused of committing several murders in the United States. Resendez was known as "the railway killer" because he allegedly traveled around the United States by freight train and com-

mitted murders near railroad lines. In early 1999, Texas police obtained a warrant for Resendez's arrest in connection with a brutal murder in Houston, Texas. The police mounted an extensive search to find Resendez and contacted several INS investigators in Houston seeking assistance in the search for him. However, none of those INS investigators placed a lookout notice' for Resendez in IDENT. Instead, the INS investigators referred the police to other agencies or databases.

Consequently, when Border Patrol agents apprehended Resendez on June 1, 1999, as he attempted to illegally cross the border into New Mexico, nothing in IDENT alerted them to the fact that Resendez was wanted for murder or had an extensive criminal record. As a result, the Border Patrol followed its standard policy and voluntarily returned Resendez to Mexico. He returned to the United States within days of his release and murdered several more people before surrendering on July 13, 1999.

The OIG review concluded that the failings by the INS employees who did not place a lookout for Resendez in IDENT were indicative of and partly caused by larger failings in the INS' s design and implementation of IDENT. We found that the training that was given to INS employees on IDENT, particularly outside the Border Patrol, was ineffective or non-existent. In the 1998 OIG report, we had noted problems with IDENT training and recommended that the INS develop and implement a strategy for sufficiently training INS personnel using IDENT. Unfortunately, the INS largely rejected this recommendation, claiming that its IDENT training was adequate. We found in the Resendez review that INS program offices, such as Investigations and Intelligence, viewed IDENT as a Border Patrol initiative and were not educated on how IDENT could be useful to their mission.

When we interviewed INS employees in various offices involved with the Resendez case, we found that their knowledge of IDENT was severely lacking. The INS investigators who were contacted by police searching for Resendez did not think of IDENT, even when they were asked to place a lookout in INS databases for Resendez. Although the INS had distributed a lookout policy, it provided no training on the policy and did little to ensure that the policy was understood or read.

IDENT was not, and still is not, linked with FBI databases. The INS's IDENT system and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the National Crime Information Center (NCIC) 2000 system were developed separately and along different time lines. Although the INS and the FBI periodically discussed integration of their systems as they were being developed, there was never a sustained effort to achieve that goal and no agreement on integration was reached. We were told that the INS and the FBI made little effort to understand the operational requirements of the other agency. Each agency focused on meeting its own requirements and did not pursue integration. As a result, when the FBI finally deployed IAFIS and NCIC 2000 in July 1999, the FBI fingerprint systems were not linked to IDENT.

The Resendez case vividly illustrated the need for integration of the INS and FBI systems and spurred the FBI and the INS to develop an integration plan. The plan required studies to help determine the feasibility of integration of the systems, which initially would allow the fingerprints of aliens apprehended by the INS to be searched against a subset of the FBI's Criminal Master File and eventually against the entire master file. However, an integration plan is still in the process of being developed and may take years to implement fully.

H. THE OIG'S "BOMBS IN BROOKLYN" REPORT

In a report issued in March 1998, the OIG examined how two individuals, Gazi Ibrahim Abu Mezer and Lafi Khalil, entered and remained in the United States before their July 1997 apprehension in Brooklyn for allegedly planning to bomb the New York City subway system. Mezer was subsequently convicted and sentenced to life imprisonment. Khalil was acquitted of charges stemming from the bombing plot but found guilty of immigration violations.

In our report, we described how both men were able to enter the United States and remain here. Khalil, who had a Jordanian passport, applied to the U.S. Consular Office in Jerusalem for a visa to travel through the United States en route to Ecuador. The consular official gave him a 29-day, C–1 transit visa after a three-minute interview. When Khalil arrived in New York on December 7, 1996, an immigration inspector mistakenly granted him a 6-month, B–2 tourist visa. He overstayed that visa and was arrested in Brooklyn, along with Mezer, in July 1997.

Mezer, who claimed Jordanian nationality, received a visa from the Canadian Embassy in Israel to study in Canada. Shortly after arriving in Canada in September 1993, he applied for convention status, which is similar to political asylum in the

United States, based on his claimed fear of persecution in Israel. Mezer later admitted that he had traveled to Canada with the intent to reach the United States.

In 1996, Mezer was detained by the Border Patrol twice while attempting to cross the border into Washington State. Each time the Border Patrol voluntarily returned him to Canada. In January 1997, the Border Patrol apprehended Mezer in Washington a third time and initiated formal deportation proceedings. Mezer then filed an application for political asylum in the United States and was later released on a $5,000 bond. In his asylum application, Mezer claimed that Israeli authorities had persecuted him because they wrongly believed he was a member of Hamas. The immigration court requested comments from the State Department about Mezer's asylum application, and the State Department returned the application with a sticker indicating that it did not have specific information on Mezer. Mezer's attorney later withdrew the asylum application, stating that Mezer had returned to Canada. Mezer was arrested shortly thereafter in Brooklyn for plotting to bomb the subway system.

During our review, we did not find any information that Mezer was a known terrorist. However, we found systemic problems that were revealed by his case. Our review found that Mezer had entered and remained in Canada despite two criminal convictions there, which highlighted the ease of entry into Canada and the difficulty of controlling illegal immigration from Canada into the United States. We also noted the inadequacy of Border Patrol resources to address illegal immigration along the northern border. In addition, Mezer's case reflected confusion between U.S. government agencies as to which agency would conduct a check for information on whether an asylum applicant was a terrorist. We recommended that the INS and the State Department coordinate more closely on accessing and sharing information that would suggest a detained alien or asylum applicant may be a terrorist.

I. FBI SYSTEMS

Findings from a July 1999 OIG report that examined aspects of the FBI's computer systems are particularly relevant in light of the ongoing terrorism investigations. In most criminal investigations—and certainly in the aftermath of the September 11 attacks—the FBI must be able to rapidly identify and disseminate pertinent intelligence information to the law enforcement community. Failure to capitalize on leads in its possession can delay or seriously impede an investigation.

In our 1999 review, the OIG examined why classified intelligence information pertaining to the Department's Campaign Finance Task Force investigation was not appropriately disseminated within the FBI and the Department and subsequently to congressional oversight committees. The OIG found that a series of problems, including deficiencies in the use and maintenance of the FBI's computer database systems, ultimately contributed to this failure.

A key feature of the FBI's Automated Case Support (ACS) system—the agency's primary case management database that contains leads and other FBI documents—is a user's ability to retrieve information regarding particular individuals, including whether they have been the subjects of other investigations. However, we found that FBI agents often did not enter important information into the database and that agents often did not conduct appropriate searches for information using the database. The end result was that the FBI could not be confident that a search for information in the ACS databases would, in fact, provide all pertinent information in the FBI's possession. In the Campaign Finance investigation, this meant that many of the documents that were later discovered regarding two key subjects of the Task Force investigation could not have been found using the FBI's databases. We found that the FBI's information management problems were caused by a variety of factors, including inappropriate policies and insufficient training, and we made recommendations to address both of these issues.

J. DOCUMENT FRAUD

While the focus of today's hearing is on technology's role in helping prevent the entry of terrorists into the United States, it is important to recognize that even if the INS or other government agencies had foolproof systems—which they do not—these systems can be defeated by document fraud. For example, visa fraud can allow terrorists and others to illegally enter the country. There is little hard data, however, to judge the magnitude of such fraud. Common types of nonimmigrant visa fraud or fraud include:

1) a person uses fraudulent documents to obtain a legitimate visa;
2) a person obtains a fraudulent visa (for example, an individual can attempt to use the passport and visa of a person who has similar looks and biographical characteristics or can purchase an altered document); or

3) an individual may not meet the spirit or intent of the specific visa program.

Historically, the OIG has played an important role in attempting to combat one aspect of immigration fraud. The OIG's Investigations Division has spent significant resources investigating immigration document-related corruption in the INS. It is important to stress that corruption by a very few INS employees should not taint the other hardworking, honest employees of the INS who faithfully perform their duties. But any such criminal conduct can affect the integrity of our lawful immigration system and, ultimately, our national security by potentially allowing criminals or terrorists to enter the country through corrupt means.

Moreover, in several reviews, the OIG has found deficient INS business practices that could open the agency to document fraud. We have found that the INS does not do a good job of safeguarding the tools used to create official documents, such as official certificates, INS authorizing stamps, and special ink. In addition, we have found that there is easy access to INS computers in order to change an entry, to order the issuance of an INS card or benefit, or to erase a disqualifying entry from an applicant's history. Computer passwords are shared and systems are unable to create an audit trail necessary to identify the users who accessed and amended a file. These deficiencies make it easier to make false computer entries that could result in the issuance of seemingly genuine INS documents.

As the INS and State Department apply greater scrutiny in adjudicating applications for nonimmigrant visas, the OIG is concerned about an increased risk of organized criminal or terrorist groups attempting to gain entry into this country by corrupting INS employees.

For the Subcommittee's information, I highlight several examples of fraud and bribery investigations worked by the OIG that involve the use of INS documents to improperly enter the country:

- Two INS immigration inspectors and two civilians were arrested on charges of conspiracy; transporting undocumented aliens; fraud and misuse of visas, permits, and other documents; and bribery. The investigation revealed that the INS employees and civilians assisted foreign nationals in entering the United States illegally by selling INS documents for $300—$500. The majority of aliens entered the United States through the INS employees' inspection lanes at the Brownsville, Texas, Port of Entry using the documents.
- A retired INS supervisory district adjudications officer in San Jose, California, a civilian immigration consultant, and a businessman each received prison sentences stemming from an extensive fraud scheme involving immigration documents. The investigation developed evidence that the adjudications officer, while working for the INS, accepted approximately $400,000 in bribes from a civilian immigration consultant and the businessman, his wife, and his sister-in-law to approve applications for permanent residency for at least 275 of their clients. The aliens entered the United States on nonimmigrant visas and the corrupt INS employee created false records in INS databases indicating that they had changed their status from "nonimmigrant" to "immigrant" (i.e., permanent resident).
- An INS immigration inspector assigned to the San Francisco International Airport was sentenced to one year in prison after pleading guilty to charges of bribery, fraud, and misuse of visas, permits, and other documents. A joint investigation by the OIG and the INS revealed that the immigration inspector stole two INS immigration stamps and two bottles of security ink and agreed to sell the items to confidential informants for $85,000. One of my concerns about this case is the fact that the INS employee was willing to sell a middleman the INS stamps and security ink without any knowledge as to the identity of intended recipient of these items.
- An INS supervisory asylum officer in New York was convicted at trial on 21 counts of bribery and obstruction of justice and was sentenced to 21 months' incarceration. A joint investigation by the OIG and the FBI revealed that the supervisory asylum officer altered hundreds of decisions in the INS' computer systems causing the original assessments written by asylum officers to change from a court referral to a grant of political asylum. Albanian and Yugoslavian nationals paid several middlemen $1,000 to $4,000 for each political asylum decision fraudulently granted by the INS supervisory asylum officer. Four middlemen and four Albanian and Yugoslavian nationals were arrested on charges of bribery, conspiracy, and document fraud.

• An INS assistant district director for examinations in New Jersey was convicted at trial and sentenced to 41 months' incarceration for document fraud and other charges. A joint OIG/FBI investigation disclosed that Lebanese nationals in the Boston area were able to obtain genuine INS advance parole documents through a middleman with an inside connection at an INS district office. The middleman fled the United States after being indicted and was a fugitive for one year. Upon his return to this country, he cooperated with the government, pleaded guilty, and identified the assistant district director as his inside connection.

• An INS immigration inspector assigned to the San Ysidro Port of Entry in southern California was sentenced to more than 12 years in prison after a federal jury convicted him for conducting a criminal enterprise through a pattern of racketeering activity, alien smuggling, and importation of controlled substances. An investigation by the San Diego Border Corruption Task Force developed evidence that the immigration inspector used his position in the INS to allow multiple loads of aliens and 3,500 pounds of marijuana to cross the border without proper inspection in exchange for approximately $350,000.

III. CONCLUSION

The issue of technology is critical to preventing terrorists from entering this country. From our past work, we have found that the INS has not managed its diverse information technology systems well, and that its systems do not do all that they should to help INS employees fulfill their critical mission. The OIG believes that the INS needs to more stringently manage and establish priorities for the development of its systems rather than spend enormous resources and effort to develop so many systems for so many different purposes.

Among other recommendations, based on our work we urge the INS and the FBI to ensure that their databases share information, both with each other and with other government agencies.

It is also abundantly clear that more resources need to be devoted to the northern border. Technology such as cameras and sensors can help in this effort, but there are too few agents and inspectors along the northern border.

The INS also must improve its tracking of nonimmigrant visa overstays. The current system for identifying overstays—manual I–94 cards inputted into the NIIS database—does not produce reliable or accurate information, either as a whole or on individual overstays, and the automated I–94 project has not worked.

We recognize that these are complex issues with no easy solutions, and that the task is enormous. It requires strategic vision, strong leadership, individual and organizational accountability, and sustained follow-through. This effort needs to be a top priority of the INS and other agencies, because effective use of technology is essential to protecting the integrity of the immigration system and the national security.

This concludes my prepared statement. I would be pleased to answer any questions.

Chairman FEINSTEIN. Thanks very much, Mr. Fine.

We will proceed along. I would like to introduce James Ziglar, who is Commissioner of the Immigration and Naturalization Service. He was confirmed to this post after distinguished service as the Senate Sergeant–At–Arms, where he managed a staff of 750 and a budget of $120 million. Today, he oversees one of the largest Federal agencies, with a staff of more than 34,000 employees and a budget in excess of $4 billion.

We welcome you, Mr. Ziglar.

STATEMENT OF JAMES W. ZIGLAR, COMMISSIONER, IMMIGRATION AND NATURALIZATION SERVICE, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. ZIGLAR. Madam Chairwoman and members of the subcommittee, I appreciate the opportunity to come today to discuss technology in terms of how we use that and employ that in our fight against terrorism.

I must add that I am always pleased to be back in the Senate. It is like home, and I am grateful for that opportunity to serve as your Sergeant at Arms for almost three years.

When I started this job two months ago, I knew I had a big challenge in front of me. Never would I have thought that things would have turned so dramatically. The goals that the President set for me and that the Senate endorsed and many of you I talked to during my confirmation process—and you set some other goals for me, also—those goals were threefold: first, to restructure the INS in a way that it would be better focused on its two missions. One is enforcement, the other one is service.

The second goal was to modernize the management structure and the processes at the INS in a way that would allow it to achieve those two goals of enforcement and service.

The third was—and this was clearly talked about at great length—to modernize, synchronize and rationalize the information technology systems at the INS in a way that, again, we could carry out our missions of enforcement and service.

Madam Chairwoman, I can tell you that those goals have not changed as a result of September 11, and the reason that they haven't changed is because an effective and an efficient INS is one of the ways, along with other Government agencies, to protect the American people against the horror that we experience on September 11.

Madam Chairwoman, I can tell you, based upon what I have learned in two months, that the INS is a willing, enthusiastic and cooperative partner in the fight against terrorism. I am firmly convinced that the INS has the will, it has the determination, and we have the human resources—we need more of them, but we have the human resources to make the changes that we need to make. And we are moving rapidly to make those changes even as we speak, and I would like to talk a little bit about some of the things we are doing.

My friend, Glenn Fine, gave you a retrospective view of the INS. I want to give you a prospective view and I want to give you a view of what we are doing today and how we are addressing some of these problems because I think—and I am deviating from notes in front of me—there is an awful lot of criticism that is absolutely justified toward the INS. Some of the criticism that is leveled at it is not justified, based upon my review of this institution, and I think we need to step back and look at what it is doing right going forward and figure out exactly how we do integrate all of these agencies and this information in an appropriate way.

Just for your information, very shortly I will be coming up here and providing you with a draft of a reorganization, restructuring plan for the INS that the Attorney General has personally approved and that is in the final stages of approval at OMB. When we are finished with it—and it is substantial and it is significant, and we have continued to develop it notwithstanding the events of September. When you see it, I think you are going to understand that we are serious about making changes at the organization, and we need your help on that.

We are at this very moment, and well before September 11, aggressively in the position of developing an information technology

enterprise architecture based upon the recommendations and the guidance and the current help from the General Accounting Office. We are hard at work with both private contractors and our people inside at developing a platform so that our technology, and our information technology especially, is integrated, the many parts of the INS, not only integrated at the INS, but we will also be integrated with other Federal organizations that we have to interact with. We are building that platform, we are designing that platform.

At the same time, we are not sitting still in terms of developing our systems. We have an investment review process there that is using what we call interim technology architecture, and it is an architecture that allows us to build pieces of this system that will fit on that enterprise architecture platform that is being developed, and will be consistent with it. So we are moving ahead even as we are developing the baseline projects that we are working on here.

Madam Chairman, with your support, we are moving ahead and will move ahead—and I know we are going to have your support on this—with the SEVIS system, and that is the student tracking system which was also known as the CIPRIS system.

As you know, and as Senator Kyl pointed out and as you pointed out, the development of a student tracking system has been the subject of much concern, opposition and other things particularly from the academic establishment, and frankly from Congress, fighting about the fees and how they are allocated and how they are collected and that sort of thing. Mysteriously, that opposition seems to have now disappeared since September 11 and we are prepared to move ahead, but we need your support.

Let me make one point about the development and deployment of the SEVIS system. As the statute is now, that system has to be funded out of the fees collected. So we have to go to the exam fee account that we have and fund it as those fees come in. That obviously means that we can only fund what we have got money to fund.

We need appropriations up front to develop that system. If we have appropriations to support it, I think we can have that system up and running in advance of the deadline that you have given us, which is December of 2002, January of 2003. I believe that we can get that done and I think we can have an effective system in place, but we need your help.

Let me talk to you a little bit about something else that we are doing at the INS that is very important, and it addresses some of the very issues that you talked about in your opening statements, all of you did, and that is that we have lots of different systems, we have lots of different information databases at the INS and they are in stovepipe form. That is true; no arguing about that.

One of the legitimate criticisms has been that we have information here and it is needed there, but there is no way of getting it there. That is true, but I am going to tell you that is not going to be true for long and it is not as true today as it was yesterday or the day before, because we are putting in place and have put in place something called the ENFORCE system.

The ENFORCE system is a general database, if you will, where all of the other databases from the INS sources will go into and are

going into, not all of them. We are putting the modules in as we speak. It also is designed to reach out to the FBI and the CIA and other sources of information, the Department of State, and bring their information into one place.

What we have also done is we have taken that and fully integrated the ENFORCE system with the IDENT system. Now, people are confused sometimes about what IDENT is. IDENT is like IAFIS; it is an identification system. It is not a database system of information about people. It is simply a system that tells you is this person who we think this person is by use of fingerprints.

So what we have done is integrate our fingerprint I.D. system with, if you will, a name and date of birth system so that once we figure out who this person is biometrically, then we can access the information, which is the way it always works. IAFIS is an identification system and it acts as NCIC.

Well, we have integrated those and we are now putting in these stovepipes, if you will, of other information into the ENFORCE system. In a very short time, we will be rolling out the first transitional work station that ultimately will integrate IDENT and IAFIS.

Senator DeWine, I know you and I have talked about this on occasion. It will integrate IDENT and IAFIS, two identification systems, so that when we have somebody come forward we have information on who that person is either from the FBI or from our files, but it is integrated. Then we will access the ENFORCE system, which is the database which draws not only from our databases internally but from the databases outside.

We have not been standing still at the INS in terms of developing these systems, and this isn't something that happened starting on September 11. This is something that was happening before September 11 and it was happening before I got there. When I got there, I came with the same assumption that we weren't doing anything and that we didn't care and all of the stuff I had been hearing.

I have done a lot of due diligence in two months and I am going to tell you there are lots of things that we need to change in this organization. But the idea that this organization is sitting around and doesn't care and hasn't been approaching these problems is not true; it is not true. We need to do a lot of things a lot better, but it is not true that we are not. We are doing that.

We are also moving forward aggressively to implement the entry/exit system. We are going to use the IBIS system, which we share with the Department of State and others, as our baseline for the entry/exit system.

Now, let me make one point, Madam Chairwoman, that you made, and that is that we have over 300 million non–U.S. citizens coming into this country every year. Two hundred-plus million of those come in through land borders. It is real easy for us to develop an entry/exit system coming through airports and seaports. I say easy. Nothing is real easy in the technology area, but it is easier. That is something that we are developing and we are going to use advance passenger information that we will put into the IBIS system and that sort of thing.

But working with the land borders is a much more difficult thing, particularly when you have land borders like Canada where have a lot of people going back and forth, and how you track them and yet not create enormous backups. So that is an issue that is going to have to be dealt with at a policy level. Systematically, we can do that. Policy-wise, that is a different issue, how we do that and balance the interests of commerce and the interests of security.

Madam Chairwoman, with your support we can do a number of things. We can complete the deployment of the border crossing card system, which we need money for. We can complete the deployment of the IDENT system, which the IG has mentioned is a good system. The failure in the IDENT system, and particularly in the Resendez case that he mentioned, was not a failure of the technology. It was a f failure of INS to train its people and to have those people understand that they need to put information into the system.

The IG testified yesterday with me and he said the IDENT system needs to be fully deployed. There is a moratorium by Congress, as you may know, on any further deployment. We have not deployed any more work stations in IDENT in two years. As a result of the Resendez case, there is a moratorium. We have 1,100 other places that we can deploy that system, but we need that moratorium lifted.

Chairman FEINSTEIN. Could you stop for a minute?

Mr. ZIGLAR. Yes, ma'am.

Chairman FEINSTEIN. You said a moratorium on deployment of IDENT?

Mr. ZIGLAR. Of the IDENT system, yes, ma'am.

Chairman FEINSTEIN. Could you explain what you mean by that?

Mr. ZIGLAR. In the appropriations process, the Congress has prohibited us from installing any more IDENT machines at any more ports of entry, and it has been on there two years. The first year, it was because of the Resendez case. The second year that it has been in effect was because until we had the IAFIS and the IDENT system integrated, you folks didn't want us to do any more.

We need to deploy 1,100 more work stations at our ports of entry so that our people have access to this, and not only at the ports of entry but also at our service centers and other places where we interview people so we can identify who these people are. We need that help.

One last thing I would like to mention, Madam Chairwoman, is something that Ambassador Ryan and I—by the way, we have worked together extremely cooperatively. Ambassador Ryan is doing a great job at the Department of State. We arrived yesterday at an agreement that we are going to deploy what is called the consolidated consular database that the Department of State has developed.

What the Department of State does is it now has a database where, when they have an application for a visa, all that information goes in there and they take a picture of this person. That picture is a digitized picture that shows up on the visa, but it is also in an electronic database. So when they issue a visa, say, in Rome, when that person shows up at Newark Airport today—and that is the only place it has been deployed on a test basis—when they

show up at Newark Airport, if they go into secondary especially, we can pull up on a screen the information from the visa and the person's picture to identify whether that is a fraudulent visa or whether that is the person.

It has worked well. It has been an experimental process that has gone on between INS and DOS. As of yesterday, Ambassador Ryan and I have agreed that we are going to deploy that, and we at INS believe that we can get this done in three months at all of our ports of entry and we are moving ahead on it. It is a done deal we start today.

Madam Chairman, I know I have gone way over my time.

Chairman FEINSTEIN. If you could wrap it up, we will move on and then have questions.

Mr. ZIGLAR. I just want you to know and I want this subcommittee to know and I want the American people to know that the INS is moving forward, and we were moving forward before September 11 and we are a full partner in this fight against terrorism.

I appreciate the opportunity to be here and I look forward to your questions.

[The prepared statement of Mr. Ziglar follows:]

STATEMENT OF JAMES W. ZIGLAR, COMMISSIONER, IMMIGRATION AND NATURALIZATION SERVICE, WASHINGTON, D.C.

Madame Chairwoman and Members of The Committee, I want to thank you for the opportunity to testify on the important issue of how technology can be better employed to prevent the entry into our country of persons who wish to do harm to our people and institutions. I am always pleased to return to the Senate. I shall always be grateful for the opportunity I had to serve as the Senate Sergeant at Arms from November 1998 to August 2001.

Although I have served as Commissioner for only two months, I have not viewed that as a liability in responding to the tragic events of September 11, primarily because of the highly professional career public servants who have provided me with mature advice and assistance. These tragic events, however, have provided an opportunity for me to examine, with a fresh eye, the management, personnel, technology, and policy needs capabilities of the INS.

STEPS TO IMPROVE SECURITY

Mr. Chairman, the questions you have—and the reason, I believe, you called this hearing—are straightforward: You and most Americans would like to know what steps we can take to improve our security consistent with our values and constitutional liberties.

Even before September 11, we were examining that question in depth at how we can improve the INS, at all levels, and especially in the area of technology. We recognize that technology is a huge "force multiplier" that we must employ effectively at the INS if we are to accomplish our mission.

Pursuant to the mandates of the Clinger-Cohen legislation, in response to the recommendations of the General Accounting Office (GAO), and because it makes good business sense, the INS is currently in the process of developing its Enterprise Architecture. This project represents our long-term, strategically-oriented approach to accomplishing the information driven aspects of the INS mission. We began the planning for this project in October 2000 and I expect the final delivery of this project, the transition plan to our target architecture, to be ready at the beginning of the 3rd quarter of FY 2002.

In addition, as part of our overall restructuring initiative, I encouraged our employees at all levels to think "outside the box" as to how we can better accomplish our mission. They responded with a number of creative ideas, some of which we are still evaluating. However, within the context of what is already known to be "doable" and effective, we have arrived are considering at a series of measures that would strengthen our enforcement capabilities. We are working within the Administration to determine how to implement these measures. Some of our ideas are as

follows: Mr. Chairman, I suggest for your consideration, and that of the entire Congress, the following actions:

BORDER PATROL

As requested in the President's budget, increase the number of Border Patrol agents and support staff along the northern border, while not neglecting the continuing needs along the southwest border. Such increases should also include necessary facilities, infrastructure and vehicles.

Provide additional agent support equipment and technology enhancements. Unfortunately, neither the Senate nor the House currently is funding the President's request at $20 million for "force multiplying technology."

> Significantly increase the number of Border Patrol agents and support staff along the northern border, while not neglecting the continued needs along the southwest border. It is important that such increases include necessary facilities infrastructure, vehicles and support personnel, and that Border Patrol personnel assigned to the northern border represents a net increase of agents nationwide.

Expand INS access to portable wireless biometric identification systems, such as mobile IDENT.

Increase funding for roads, lights, fences, and vehicle barriers.

INSPECTIONS

In the Inspections area, as we proposed in our FY 2002 budget, we believe we should increase the number of Inspectors at our Ports of Entry.

In the Inspections area, increase the number of inspectors to fully staff land borders, airports, and seaports, allowing our ports-of-entry to operate without jeopardizing security or officer safety.

Require inspection of all International-to-International Transit Passengers (ITI) so that all travelers who arrive in the United States are inspected.

Increase the number of criminal investigators and intelligence analysts to enhance investigative capabilities and develop more information on possible national security threats. A substantially enhanced investigative and intelligence force would make it possible to begin to address the concern about nonimmigrants who illegally enter, overstay or otherwise violate the immigration laws of the United States.

INFORMATION AND TECHNOLOGY INITIATIVES

Require carriers to submit Advance Passenger Information before boarding passengers (whether the passenger is heading to the United States or attempting to depart the United States) to assist in preventing known or suspected terrorists, criminals, and inadmissible passengers from boarding.

Make Advance Passenger Information data widely available to law enforcement agencies, enhancing the ability to identify potential threats prior to departure from or arrival in the United States, as well as to prevent the departure of individuals who may have committed crimes while in the United States. This would require additional personnel and equipment.

Implement the National Crime Information Center Interstate Identification Index (NCIC III) at all ports of entry so that aliens with criminal histories can be identified prior to or upon arrival in the United States. NCIC III should also be available at all consular posts, INS service centers and adjudication offices to help identify aliens who pose a potential threat.

Improve lookout system checks for the adjudications of applications at INS service centers. This would require additional personnel.

Improve INS infrastructure and integration of all data systems so that data from all sources on aliens is accessible to inspectors, special agents, adjudicators, and other appropriate law enforcement agencies. This initiative is ongoing.

but will require substantial investment to complete.

PERSONNEL ISSUES

Provide statutory authority to waive the calendar-year overtime cap for INS employees to increase the number of staff-hours available by increasing the overtime hours people can work. This proposal is included in the Administration's Terrorism Bill.

OTHER INITIATIVES This onerous provision that has not been imposed on most other federal agencies has created a serious problem during the current heightened security posture. For example, the continued availability of Border Patrol Agents for security at major airports is significantly impacted by this provisio

Re-examine and potentially eliminate the Transit Without Visa Program (TWOV) and Progressive Clearance to prevent inadmissible international passengers from entering the United States.

Reassess the designation of specific countries in the Visa Waiver Program to ensure that proper passport policies are in place. This initiative will require the concurrence of and joint participation by the Department of State.

Obtain from the Department of State visa data and photographs in electronic form at ports of entry so that visa information will be available at the time of actual inspection.

Explore alternative inspection systems that allow for facilitation of low risk travelers while focusing on high-risk travelers.

And review the present listing of designated ports of entry, in concert with the U.S. Customs Service, to eliminate unnecessary ports. This will allow the INS to deploy more inspectors to fewer locations making for a more efficient use of resources.

DATABASE IMPROVEMENTS

In addition to the measures cited above, I have instructed my staff to move forward expeditiously on two database improvement projects mandated by Congress. While neither is a panacea, both would be an improvement over the status quo. First, there has been much attention paid to student visas in recent weeks. Today, the INS maintains limited records on foreign students and is able to access that information on demand. However, the information is on old technology platforms that are insufficient for today's need for rapid access. That is why we are moving forward with the Student Exchange Visitor Information System (SEVIS), formerly known as CIPRIS. Objections, primarily by the academic establishment, have delayed its development and deployment. However, with the events of September 11, that objection has virtually disappeared and the INS, with your help, will meet, and intends to beat, the Congress' date of December 20, 2003 to start implementation of SEVIS with respect to all foreign nationals holding student visas. I hasten to add that there is a critical need to concurrently review and revise the process by which foreign students gain admission to the United States through the so-called I–20 certification process as we build the system. To revise and rationalize this process will require cooperation between the Department of State and the INS.

Second, substantial attention also has been paid to entry and exit data. Currently, the INS collects data on the entry and exit of certain visitors. The data, most of which is provided to the INS in paper form to meet our manifest requirements, first must be transferred by hand from paper to an electronic database. This is an extremely inefficient way of processing data which delays access to the data by weeks and months. Knowing who has entered and who has departed our country in real time is an important element in enforcing our laws. The Data Management Improvement Act, passed in 2000, requires the INS to develop a fully-automated integrated entry-exit data collection system and deploy this system at airports and seaports by the end of 2003, the 50 largest land ports of entry by the end of 2004, and completing the deployment to all other ports of entry by the end of 2005. The legislation also requires a private sector role to ensure that any systems developed to collect data do not harm tourism or trade. The INS is moving forward to meet, or beat, those deadlines.

The INS already uses limited airline and cruise line data that is now provided voluntarily as an integral part of the inspection process at airports and seaports. We will work closely with Congress, other agencies, and the travel industry in the coming months to expand our access to needed data and to enhance our use of that data to ensure border security and more complete tracking of arrivals and departures.

There has also been a great deal of focus on the databases used to identify persons who are inadmissible to the United States or who pose a threat to our country. The INS, the Customs Service, and the Department of State's Bureau of Consular Affairs have worked diligently over the past decade to provide our ports of entry and consular posts with access to data needed by our officers. The data contained in the National Automated Immigration Lookout System (NAILS), the Treasury Enforcement Communications System (TECS II), and the Consular Lookout and Support System (CLASS) are uniformly available to our ports of entry through a shared database called the Interagency Border Inspection System (IBIS) that is maintained on the U.S. Customs Service mainframe computer.

Through IBIS, the officers at our ports of entry can also access limited data from the National Crime Information Center (NCIC). Immigration and Customs officers have long had the capability to check NCIC wanted persons data on a limited basis.

Only recently have immigration inspectors been authorized to routinely use NCIC criminal history data (NCIC III) to identify criminal aliens in advance of their arrival. This capacity now exists at two ports of entry. Before September 11, the INS was working to expand the availability of this valuable data source to additional locations. Legislation is being considered to ensure this expansion is successful. I strongly support this legislation. To expedite this process, we will require the assistance of Congress for additional communications and mainframe capacity so that we may obtain real-time NCIC III data.

Many people who cross our land borders do so with a Border Crossing Card (BCC). The INS and State Department have been working aggressively over the past several years to replace the old Border Crossing Cards with the new biometric "laser visa." Based on the statutory deadline, holders of the old BCC can no longer enter the country. The new BCC has many security features that make it a much more secure entry document.

Both at and between our ports of entry, the INS has used a fingerprint identification system known as IDENT to track immigration violators. This system has provided the INS with a significant capacity to identify recidivists and impostors. Congress has directed the Department of Justice to integrate IDENT with access to the FBI's automated fingerprint system, IAFIS, and we have been proceeding toward that objective with the FBI and under the Department's direction.

THE LIMITS OF TECHNOLOGY

There is no quick fix, technological or otherwise, to the problems we face. We must work with advanced technology and do all we can to improve our systems. But we should not mislead ourselves into thinking that technology alone can solve our problems. Technology must be coupled with a strong intelligence and information-gathering and distribution system if we are to leverage our resources and maximize our capabilities. That will require the seamless cooperation among the many government agencies involved.

It should be noted that more than five hundred million inspections are conducted at our ports of entry every year, and hundreds of millions of people enter the United States without visas, either because they are U.S. citizens, through visa waiver programs, or other exemptions from the normal visa process; the INS has only 4,775 Inspectors to process these hundreds of millions of visitors and approximately 2,000 investigators and intelligence agents throughout the country who are available to deal with persons who have entered illegally, are criminal aliens, or have overstayed their visas or otherwise have violated the terms of their status as visitors in the United States.

If we are to meet the challenges of the future, we need to make changes at the INS and we are in the process of making those changes. The structure of the organization and the management systems that we have in place are outdated and, in many respects, inadequate for the challenges we face. Our information technology systems and related processes must be improved in order to ensure timely and accurate determinations with respect to those who wish to enter our country and those who wish to apply for benefits under our immigrations laws. The management restructuring of the INS is on its way—a mandate the President and the Congress have given me—and the improvement of our information technology systems is moving ahead and can be accomplished with the help and support of Congress.

Madame Chairwoman, I would like to say one word about INS employees and the events of September 11. Within hours of the attacks, the INS was working closely with the FBI to help determine who perpetrated these crimes and to bring those people to justice. Within 24 hours, under "Operation Safe Passage," The INS deployed several hundred Border Patrol agents to eight major U.S. airports to increase security, prevent further terrorist incidents and restore a sense of trust to the traveling public. At America's ports of entry, INS inspectors continue to work tirelessly to inspect arriving visitors, while ensuring the flow of legitimate commerce and tourism. Meanwhile, despite the tragedies and the disruptions, our service operations have managed to complete over 35,000 naturalizations nationwide and process thousands of other applications since September 11. America should be proud of the extraordinary effort of these men and women.

LOOKING AHEAD

It has been said that after September 11 "everything has changed." I hope that is not true. America must remain America, a symbol of freedom and a beacon of hope to those who seek a better life for themselves and their children. We must increase our security and improve our systems but in doing so we must not forget what has made this nation great—our openness to new ideas and new people, and

a commitment to individual freedom, shared values, innovation and the free market. If, in response to the events of September 11., we engage in excess and shut out what has made America great, then we will have given the terrorists a far greater victory than they could have hoped to achieve.

Thank you for this opportunity to appear, Madame Chairwoman. I look forward to your questions.

Chairman FEINSTEIN. Thank you very much.

I would like to acknowledge the fact that Senator Cantwell has joined the subcommittee.

Perhaps after Mary Ryan testifies, if you have some comments you would like to make, we will go to you.

Let me properly introduce you. Mary Ryan is Assistant Secretary of State for Consular Affairs. She entered the Foreign Service in 1966 and has had a long and distinguished career at the State Department. In her post, Ambassador Ryan is charged with overseeing the issuance of visas to foreigners wishing to enter the United States. She assumed these duties in 1993.

Welcome, Ms. Ryan.

STATEMENT OF MARY A. RYAN, ASSISTANT SECRETARY FOR CONSULAR AFFAIRS, DEPARTMENT OF STATE, WASHINGTON, D.C.

Ms. RYAN. Thank you, Madam Chairwoman, members of the subcommittee. I appreciate the opportunity to appear before you today to explain the role of the Bureau of Consular Affairs, and most particularly our visa processing system, in our country's border security program.

I have a longer statement which I would like to submit for the record, if I have your permission.

Chairman FEINSTEIN. Please. Thank you.

Ms. RYAN. The resolve of the Department of State and the Bureau of Consular Affairs to be full partners in the war against terrorism is stronger than ever. In my testimony today, Madam Chair, I will describe what we are doing to make our consular name check systems the best in the world and our plans to make them even better in the future. I will also address procedures for visa issuance and the scope of the Department's data-sharing with intelligence and law enforcement communities.

One of the points that I want to stress most especially to all of you here in the subcommittee is that we must have information. We are only as good as the information that goes into the system. If we have no information on the aliens from other agencies, then the name check system is not as good as it could be. So if there is one point that I can leave with this subcommittee today, it is that we must have more information-sharing.

I can say with confidence that we are using today a state-of-the-art visa name check system and we continue to seek and exploit new technologies to strengthen our capabilities.

Let me begin by noting that all visa cases are processed by using automated systems which prompt a name check through the Department of State's centralized lookout system known as CLASS. A consular officer must review all hits before the case can be formally approved for printing. There is no override to this feature. Simply stated, it is not possible to issue a visa unless the name check has been completed and reviewed by an officer.

The Department also has in place special headquarters clearance procedures for nationals of certain countries, including students, such as those on the State Sponsors of Terrorism list, as well as for those whose planned travel raises concerns about unauthorized access to sensitive technologies.

Once approved, a visa containing numerous security features and a digitized photo is placed in the alien's passport. Now, I point out that the validity of the visa has nothing to do with the period for which the alien may remain in the United States. What a visa does is to allow the alien to apply at the port of entry for admission to the United States, and INS only may authorize such entry and INS determines how long the alien can stay in the United States.

I want to describe our name check database for you. CLASS, which stands for the Consular Lookout and Support System, contains about 5.7 million records concerning foreigners, most of which originate with visa applications at our consulates and embassies overseas. But INS, DEA, the Department of Justice and other Federal agencies also contribute to our system. We, in turn, provided approximately 500,000 lookout records to other agencies through real-time electronic links to the Interagency Border Inspection System which the Commissioner mentioned, the IBIS system.

In the aftermath of the 1993 World Trade Center bombing, the Bureau of Consular Affairs funded a counterterrorism tool called TIPOFF. This utilizes sensitive intelligence and law enforcement information from the CIA, from the NSA and from the FBI and from our overseas posts concerning known or suspected terrorists.

The TIPOFF staff screens all incoming intelligence reports and other sources of information for the names and biographic data of known or suspected terrorists. Permission is obtained from the relevant agencies to declassify identifying data of suspected terrorists and that data is then entered into the CLASS system and into IBIS.

We also have a program which we call Visas Viper, another integral part of the TIPOFF system. The Visas Viper staff, in close coordination with the Bureau of Consular Affairs, solicits information on suspected terrorists from overseas posts for inclusion in this database.

Beginning in 1996, with the help of Congress through the retained machine-readable visa fees, Consular Affairs undertook a major modernization of our systems. By 2001, all visa data collected abroad, including photos of the applicants, was being replicated to the consular consolidated database and made available to posts abroad.

This year, we deployed a pilot program to share limited non-immigrant visa data with INS inspectors at Newark. We are very pleased that INS will soon expand the use of this replicated data to all ports of entry. This will provide each INS inspector with a photo to compare with the person in front of them, a system cheaper than fingerprints and just as effective. In the meantime, INS inspectors have access to our electronic database through the INS Forensic Documents Laboratory.

The Consular Lookout and Support System is modern and it is extendable. Our name check system remains robust because we

continue to upgrade it. Let me give you a few of the initiatives underway related to this goal.

For many years, we sought access to FBI criminal records data on aliens applying for non-immigrant visas, and I am very grateful to the members of Congress that legislation has been introduced finally in both Houses that would permit us access to this data.

We will soon introduce an improved field backup name check system for use when the telecommunications links are interrupted. By the summer of 2002, every visa processing post will have a local backup that closely approximates the abilities of the CLASS mainframe.

Photographs are our key to our exploration of biometrics. Because very visa application contains a photograph, we already capture a biometric identifier for all applicants. For this reason, we have been for some time investigating the use of facial recognition technology for identification purposes.

Pilots at posts in India and Nigeria have proven very promising, and in late August we launched a pilot at the Kentucky consumer center aimed at detecting invalid diversity visa applications. We will soon the test the abilities of facial recognition software to compare visa applicants to a sample database of photographs of suspected terrorists. We seek to expand the pool of such photographs through liaison with other Government agencies, and we are also consulting with the private sector on facial recognition technology.

We will soon complete field-testing a new, more secure non-immigrant visa, and design a machine-readable secure immigrant visa that will, in conjunction with the data share program, virtually eliminate photo substitution. We are planning to develop a forensic documents laboratory in the Bureau of Consular Affairs to give us an independent capacity to detect and counter fraudulent or counterfeit U.S. and foreign visas and passports.

Madam Chairwoman, all of these initiatives, past, present and future, have been made possible through a very wise decision by the Congress a few years ago to permit us to retain a machine-readable visa fee. Since 1994, when we were given this authorization to charge and to keep the fee, we have spent every penny sensibly and judiciously.

We continue to rely upon machine-readable visa fees to finance the salary and basic benefits of virtually all American employees who provide consular services. Permanent and uncapped MRV fees are essential to continuing our efforts to enhance our Nation's border security.

Madam Chairwoman, in our free society we must continue improving the security of our borders, while keeping our hearts and our minds and our economy open to new people, to new ideas, and to new markets. The Bureau of Consular Affairs has been, and will continue to be a full partner in the battle against terrorism.

I close with the point that I made at the outset. We cannot be the effective outer ring of border security if we do not get information on people who seek to harm our country from the intelligence and law enforcement agencies. Information-sharing is key to our protecting our Nation.

Thank you, Madam Chairwoman and members of the subcommittee, for the opportunity to appear before you and I would be happy to try to answer any questions that you might have.

[The prepared statement of Ms. Ryan follows:]

STATEMENT OF MARY A. RYAN, ASSISTANT SECRETARY FOR CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE, WASHINGTON, D.C.

Madam Chair and Members of the Committee:

Thank you for the opportunity to appear before you today to explain the role of the Bureau of Consular Affairs, and most particularly our visa processing system, in this country's border security program. I only wish, Madam Chair, that the context for this hearing could be different. In that case I could open these remarks by saying how happy I am to appear before you, because I am proud of the systems we have developed over the past several years and that we work very hard to improve each and every day. I would convey again my appreciation for the help that the Congress has given the Department to improve our consular systems by allowing us to retain machine-readable visa (MRV) fees. However, I appear before you today keenly aware of the terrible tragedy that befell our country and all civilized countries on September 11.

In my testimony, Madam Chair, I will outline for you what we have been doing to make our consular systems the best in the world and our plans to make those systems even better in the future. During my tenure as Assistant Secretary, the Bureau of Consular Affairs (CA) has been continually engaged in efforts to design, deploy, and improve the systems that help flag for our consular officers terrorists and criminals among visa applicants. I can say with confidence that ours is a state-of-the-art system that functions as it was designed. At the same time, we continue to seek and exploit new technologies to strengthen our capabilities. If there is any single point I can leave with the committee, it is that that any namecheck system is and will be only as good as the information we receive to put in it.

VISA PROCESSING

I will first focus on non-immigrant visa processing and explain briefly how applicants are processed so that you will understand the environment in which our systems operate. Applicants for non-immigrant visas submit a written application, with a passport and photo, for adjudication by a commissioned consular officer or other designated U.S. citizen. Locally engaged staff assist in visa processing but are not authorized to approve and issue visas.

Visa applications are processed using sophisticated automated systems. Data entry automatically prompts a namecheck through the Department of State's centralized lookout system (CLASS, the details of which I will discuss later in my testimony). A consular officer must review all hits before the case can be formally approved for printing. There is no override for this feature; it is not possible to print a visa unless a namecheck has been completed and reviewed by an officer.

Consular officers evaluate applications by looking at the full range of criteria established by U.S. immigration law. They review the credibility of professed plans for travel to the U.S. For most visas, applicants must establish that they intend to visit the U.S. only temporarily, are qualified for the visa classification sought, and will undertake only activities consistent with the particular visa status. Applicants must also establish that they are not otherwise ineligible to receive a visa under one of the specific grounds of ineligibility in the Immigration and Nationality Act, including terrorism, drug trafficking and alien smuggling.

In addition to namecheck results, consular officers use a combination of experience, knowledge of local economic, political and cultural conditions, and common sense to evaluate applications. Supporting documentation may be solicited and reviewed as needed. When there are specific signs of fraud or deception, an investigation may be conducted using consular anti-fraud resources.

The ever-growing numbers of visa applications has meant that consular officers must reach decisions in individual cases rapidly. To assist them in doing so, our namecheck technology provides results in real-time. We have used outside linguistic experts to make our search criteria for "hits" as helpful as possible. We have instituted sophisticated Arabic and Russian/Slavic algorithms to identify names regardless of transliteration variations, and are presently developing a similar algorithm for Hispanic names.

Once approved, a visa containing numerous security features and a digitized photo is placed in the alien's passport. The maximum period of visa validity is ten years for multiple entries. The validities of different types of non-immigrant visas

are determined on the basis of reciprocity with each foreign government. I should point out, Madame Chair, that the period of visa validity has nothing to do with the period for which an alien may remain in the United States. A visa permits an alien to apply for entry to the U.S., but only the INS may authorize such entry and determine the alien's length of stay.

Visa data, including photos and pertinent biographic data, is electronically forwarded to the Consolidated Consular Database maintained in Washington. This database also contains information on refused applications.

Immigrant visas are for persons intending to reside permanently in the United States. U.S. citizens and legal permanent resident aliens, as well as prospective employers, file with the INS petitions on behalf of certain relatives and employees. A special element of U.S. immigration law is the Diversity Visa (DV) for which "winners" are chosen by lottery. Like non-immigrant visa applicants, immigrant visa and DV applicants must undergo namechecks. In addition, an FBI employee at the National Visa Center does a National Criminal Information Center (NCIC) criminal history check of these applicants.

I should note that, while immigrants are covered by NCIC screening, non-immigrants are not. I'll return to the solution to this problem, which I hope is imminent, in the context of our namecheck system.

THE NAMECHECK SYSTEM

Integral to visa processing is the namecheck system. CA is well aware of the importance of sharing and receiving critical intelligence and criminal data from intelligence and law enforcement agencies. In addition to ensuring that no visa is issued without a namecheck, we have worked hard over the past decade to deliver more information from other agencies to our visa officers via the namecheck system.

Our lookout database, the Consular Lookout and Support System (CLASS), contains about 5.7 million records on foreigners, most of which originate with the visa application process at our consulates and embassies overseas. A variety of federal agencies contribute lookouts to our system. INS has provided over one million records, and DEA about 330,000. Customs is working with us to provide 20,000 or more lookouts from its serious drug violator records by the end of this year. We in turn provide Customs, INS and other agencies using the Interagency Border Inspection System (IBIS) with approximately 500,000 lookout records through a real-time electronic link.

We also provide our officers, and the INS, with data on lost and stolen foreign passports to prevent the use of such passports by impostors.

TIPOFF AND VISAS VIPER

In the aftermath of the 1993 World Trade Center bombing, the Bureau of Consular Affairs—as part of the Department of State's border security program—funded a border security and counterterrorism tool known as TIPOFF. It was developed, and is managed, by the Bureau of Intelligence and Research (INR), utilizing sensitive intelligence and law enforcement information from the CIA, NSA, FBI and our overseas posts concerning known or suspected terrorists. TIPOFF's objective is to detect these individuals either as they apply for visas overseas, or as they attempt to pass through U.S., Canadian, and Australian border entry posts. (Data-sharing programs were implemented with Canada in 1997, and with Australia in 2000.)

The TIPOFF staff in INR screens all incoming intelligence reports, embassy cables and other sources of information for those documents containing the names and biographic data of known or suspected terrorists. Following strict procedures approved by the respective intelligence and law enforcement agencies, permission is obtained to declassify names, nationalities, passport numbers and dates of birth of suspected terrorists. This data is then entered into CLASS and the INS and Custom Service's IBIS system. Consular officers overseas encounter "hits" based on TIPOFF data in the regular course of their work. The CLASS database contains over 48,000 such records. TIPOFF has passed approximately 23,000 records to INS and other inspection services at ports of entry via IBIS, which uses a higher standard of biographic data for its entries.

The Visas Viper program is an integral part of TIPOFF. The TIPOFF/Viper staff works in close coordination with CA to solicit information about suspected terrorists from overseas posts. This data is included in the TIPOFF database and watchlisted in CLASS and IBIS. A procedural adjunct to the Visas Viper program, called TIPPIX, incorporates terrorists' photographs into the TIPOFF and IBIS databases.

TIPOFF performs the following important functions:

It helps preclude the inadvertent issuance of visas to terrorists whose names are known to intelligence and law enforcement agencies; It warns embassies and consulates that certain applicants may pose a security risk;
It alerts intelligence and law enforcement agencies that a suspected terrorist is applying for a visa;
It provides a means for informed decisions to be made on whether to issue a visa for operational or other policy considerations, or deny the application;
It enables INS and Customs to detect suspected terrorists who may have obtained a visa prior to being watchlisted in CLASS, or who are attempting to enter the U.S. through the Visa Waiver Program (VWP);
And it provides operational opportunities at border entry points through use of "silent hits" or other handling codes.

We are also comparing new TIPOFF hits in the Consular Lookout and Support System with visa issuance information in the Consolidated Consular Database, to determine if a subject of derogatory information was issued a visa before the hit was created.

SECURITY ADVISORY OPINIONS

We also address cases posing potential security threats using Security Advisory Opinion procedures. We have concluded a series of agreements with law enforcement and national security agencies concerning categories of individuals of concern. Such persons are the subjects of a cable prepared by a consular officer and disseminated electronically to all appropriate agencies for an in-depth clearance.

The Department of State has designated Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria as state sponsors of terrorism. Visa applications by officials and diplomats of these countries for the most part must be submitted to the Visa Office for review and an advisory opinion as to ineligibility before a visa can be issued. (This requirement does not presently extend to diplomatic/official visa applicants from Syria.) Non-official visa applicants from these countries are also subject to a wide range of special clearance procedures based on their background, the nature of their proposed visit, and the type of visa they are seeking.

Based on agreements with the FBI, we also maintain a variety of special clearance procedures—beyond the regular CLASS namecheck—for numerous other nationalities, including Afghanistan. The reasons for these special clearance procedures vary, but include concerns related to espionage, technology transfer, economic sanctions, and human rights violations.

In addition to these nationality-specific clearance requirements, we universally require special clearance for applicants of any nationality who are the subject of the most serious CLASS lookouts. We similarly require special clearance for applicants whose planned travel to the United States raises concerns about unauthorized access to sensitive technologies, even if there is no lookout entry for the individual. Consular officers are also asked to submit for a security advisory opinion any other cases that they feel raise security concerns, regardless of namecheck results.

THE CONSULAR CONSOLIDATED DATABASE

Our data-sharing efforts are not, however, limited to the namecheck system. We are now delivering more information to our visa officers via a globalized database of visa records. Beginning in 1996, thanks to the help of Congress with retained MRV fees, Consular Affairs undertook major modernization of our systems. By March 2001, all visa data collected abroad was being replicated to the Consular Consolidated Database. In May 2001, we made the Consular Consolidated Database available to all our visa officers abroad. The photo and details of visa issuance, once only available locally to the post taking action, are now available in real-time to all visa offices worldwide. Visas can be checked at any point in the issuance process against all issued and refused visas worldwide, and consular management in Washington now has access to up-to-the-minute information about visa and passport issuance around the world.

DATA-SHARING WITH THE INS AND OTHER FEDERAL INSPECTION SERVICES

We are working to widen the flow of information to relevant Federal Inspection Services. We are mindful of the challenges that INS faces in inspecting millions of foreign visitors at ports of entry. We have a number of initiatives underway to share additional information with INS in order to improve border security. As I mentioned earlier, the Consolidated Consular Database allows us to make visa information, including digital non-immigrant visa photographs, immediately available both in Washington and at all consular sections worldwide. We want INS to be able to make

good use of this data, in particular photos of each individual who has been issued a visa.

Since the mid-1990's, State and INS have had a cooperative program which has resulted in State forwarding to INS, for use at ports of entry, electronic data on 55% of all immigrant visa recipients. The two agencies have cooperated in exchanging information at all stages of the immigrant visa process, from approving petitions to issuing legal permanent residence cards. We are about to make certain software changes that should allow complete sharing of immigrant visa information with INS within the next year.

The Department has for some time been prepared to share all of its replicated non-immigrant visa files with INS as soon as the Service is ready to receive it. Towards that end, in July 2001, we deployed a pilot program to share limited non-immigrant visa data with INS inspectors at Newark and with the INS forensic document lab. The program was expanded to Miami in September, and INS will make the data available to several other ports of entry soon. We look forward to the day when we can share this information will all INS ports of entry, as it will give INS inspectors near real-time access to data that will allow them to better detect fraud and facilitate legitimate travelers. In the meantime, INS inspectors have access to our electronic visa data via telephone contact with the Visa Office

LOOKING AHEAD: IMPROVING AND EXTENDING OUR SYSTEMS

The Bureau of Consular Affairs has staff specifically dedicated to technical development to ensure we maintain state-of-the-art tools for adjudicating visas. The Consular Lookout and Support System is modern and extendible. Our namecheck system remains robust because we continue to upgrade it. We are committed and are actively working to expand datasharing with INS, other federal inspection services and law enforcement agencies.

A. Gaining Access to FBI NCIC III Data

We need access to FBI criminal record data (NCIC III) on aliens to assist consular officers in their adjudication of visa applications and have been seeking authority for such access for many years. We already screen our immigrant applicants using FBI information and want to do the same for non-immigrant applicants. We envision a system of index records on aliens (excluding all U.S. citizens and legal permanent residents) that is added directly to the CLASS lookout system and that will signal there may be derogatory FBI information on an applicant. I am grateful to Members of Congress that this legislation has been introduced in both Houses of Congress. We appreciate the support of Congress on this important legislation.

B. Short-term improvements to Visa Systems

This winter we will introduce improved field backup namecheck systems. By summer 2002 we plan to deploy a "real time update" feature for these systems that will give every visa processing post a local back-up that closely approaches the abilities of CLASS mainframe.

Before the end of this year, we will modify our existing database of lost and stolen blank foreign passports to accommodate entries by Foreign Service posts of individual, foreign passports that are reported as lost or stolen. Lost and stolen passport data will continue to be shared with federal inspection agencies through IBIS.

Specific enhancements aimed at giving visa officers more detailed lookout information have been in the works over the past year. By spring 2002, we will deploy features in our nonimmigrant visa system that will increase the scope of data associated with our lookout entries. Using scanning, we will begin augmenting the lookouts with global, electronic access to refusal files (and photos) now kept at individual Foreign Service posts.

C. Facial Recognition

As I have said, Madame Chair, every visa application contains a photograph, which means we already capture a biometric indicator for every applicant. Accordingly, we have been investigating the use of emerging facial recognition technology in the consular business process.

Evaluations comparing non-immigrant visa photos at posts in India and Nigeria proved promising in identifying impostors presenting fraudulent applications. In late August, we launched a pilot at the Kentucky Consular Center for Diversity Visas aimed at detecting invalid applications from persons working around our procedures. We will soon test the capability of facial recognition software to compare a sample database of photographs of suspected terrorists to those of visa applicants. We seek to expand the pool of photographs available for this use through efforts with other USG agencies.

D. Document Security

We soon will complete field-testing a new, more secure non-immigrant visa. Laboratory tests have shown that it is much more tamper-resistant than the current version. We will also complete design of a machine-readable, secure immigrant visa that will, in conjunction with the data-share program, virtually eliminate photo-substitution. We will provide our consulates with special secure ink with which to cancel visas, so that efforts to "wash" or "recycle" genuine visas will be much more difficult.

We are planning to develop within the Bureau of Consular Affairs an independent capacity to detect and counter fraudulent or counterfeit U.S. and foreign visas and passports by creating a new office built around a forensic document laboratory. This office also would coordinate all Bureau efforts to assess biometrics technologies.

E. Human Resources

Using MRV fees, the Department currently funds the salaries and benefits of 2,130 full-time positions. MRV funds will also be required to increase consular staffing worldwide, to address growing demands in the visa adjudication process. We are committed to an effective training program for consular employees, including an intensive one-week training course for consular field officers on namecheck systems and linguistic concepts.

MACHINE-READABLE VISA FEES PROVIDE THE MEANS FOR IMPROVEMENTS

Madam Chair, all of these initiatives—past, present and future—have been made possible because of a very wise decision by Congress a few years ago to permit us to retain machine-readable visa (MRV) fees. Since 1994, we have spent every penny of these fees sensibly and judiciously. As I mentioned, the Bureau of Consular Affairs relies upon MRV fees to finance the salary and basic benefits of virtually all American employees who provide worldwide consular services as well as to make improvements to our systems. Permanent and uncapped MRV fees are essential to continuing our efforts to enhance the nation's Border Security Program. With this funding authority, we can ensure we have sufficient personnel to cover staffing and training gaps and to help meet peak season workloads. We can also adjust staffing to compensate for additional anticipated steps in the visa adjudication process and other changes to increase security.

This funding allowed us to modernize our consular systems, and some of our future proceeds will go into further system upgrades, such as the scanning of our refusal files to augment lookout information. Other major expenditures looming include establishing additional back-up capabilities for the sophisticated automated systems that support both CLASS and the Consolidated Consular Database.

The level of resources available to federal border agencies greatly affects our progress, particularly in interagency sharing of visa information. We must continue to work closely with other agencies on data-sharing to ensure full access to information for consular officers. We are anxious to provide visa data to federal inspection services and would like to see more rapid progress. Modernization of other agencies' systems—including more modern protocols in data exchange and more secure, flexible connectivity—is key to significant progress. We actively participate in the Border Agency Partnership (formerly IBIS), which aims to tackle these problems.

CLOSING

Madam Chair, we live in a free and open society. These characteristics, so precious to all Americans, make our country a magnet to those who seek greater political, economic and social opportunities, as well as a target for those who hate us and seek to do us harm. We must continue improving the security of our borders while keeping our hearts and our economy open to new people, ideas and markets. CA has been and will continue to be a full partner in the battle against terrorism. Although the freedom and openness we value so much make totally foolproof systems virtually impossible, I am confident that our current system is state-of-the-art and functions as it was designed. I am also confident that we are on the right track with our efforts to find new technologies and institute data-sharing arrangements with other agencies.

I close, Madam Chair, with the point I made at the outset of these remarks—the effectiveness and success of our systems rely not only on the quantity, but also on the quality and timeliness of the information that goes into it.

Thank you, Madam Chair and members of the committee, for permitting me to share my thoughts with you today. I would now be pleased to answer any questions you have for me.

Chairman FEINSTEIN. Thanks very much, Ambassador Ryan.

What I would like to do now is have a brief opening statement from Senator Cantwell and then we will begin the questions.

Senator Cantwell?

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

Senator CANTWELL. Thank you, Madam Chair, and I do want to express my great appreciation to you and to Senator Kyl for your longstanding interest in this issue and your work. Clearly, this hearing is a product of not just a reaction to September 11, but a tremendous amount of work and focus by this subcommittee, and I applaud you for that and the legislation that you have put forth in the past.

To the people that we are hearing from today, obviously the message is not that we haven't been doing anything. The message is that we need to move faster, and you have articulated some of the ways in which we need to move faster.

Clearly, Congress has not always been consistent in the message as it relates to immigration and our borders, and hopefully this committee can play a leadership role in making sure that our colleagues realize that if we are going to be effective in this area, we need to send a consistent and effective message, and the resources to go along with that.

Last night, we passed major anti-terrorism legislation that contained a specific new tool, a requirement that State and Justice develop a visa standard to secure our borders and to make sure that individuals who are seeking entry into our country can be identified, and that that information can be used in a system that makes sure that people who have known activities are kept out of our country.

Having had the Ressam case in the Northwest where someone entered Canada on falsified papers and was detained but was successful enough after being detained to create a new identity by getting a Canadian birth certificate and then getting a Canadian passport and, in reality, loading up a vehicle with explosives and then traveling to the Blaine border in Washington State, we have a situation here where we have to have a system that is focused on point of origin, not point of entry.

We need to be able to track people with certainty, not 100-percent certainty that their name and identification absolutely match at that point, but at point of origin knowing exactly who we are dealing with at that point by a biometric standard that then can be used to track these individuals on their various routes from that point.

I believe that citizenship in our country has its privileges, and those privileges are the right to privacy. Those individuals who are seeking access to our country should also have the responsibility of providing us with the information that we need to make sure that our borders are safe.

So I appreciate the attention that all of you are giving to this critical issue, and the challenge that you all have on your shoulders, given the recent responsibilities in this new post and the

huge history that we all have to deal with in this legacy of not being able to adequate meet the hurdles that are before us.

So I look forward with enthusiasm to working with all of you and this subcommittee on this very challenging issue about how we focus our anti-terrorist activities on making sure that we do a better job abroad, giving access only to those people that we know we can have some data and background on their activities, and making sure that that system is fool-proof.

Thank you, Madam Chairman.

Chairman FEINSTEIN. Thanks very much, Senator Cantwell.

Let us now proceed with the questions. If it is agreeable, I would suggest five-minute rounds and if we need a second round, we can go ahead and do that.

Mr. Fine, I would like to ask you this question. Do you believe that the dangers presented by the visa waiver program, particularly in light of the recent attacks, warrant its continued existence as currently structured?

Mr. FINE. Senator Feinstein, that is a difficult question. It does allow the flow of individuals more freely into the United States, but it creates incredible risks that the inspectors at the port of entry do not have adequate information about suspected terrorists, criminals and others who should not be here.

I think we need to look at that program, and one thing we need to look at is whether the countries that are participating in it are providing sufficient information to us, information about intelligence about the suspected terrorists, machine-readable passports, biometric information about their individuals. I would suggest that we look at that before canceling the program totally, but there does need to be significant attention paid to that program.

Another issue is—

Chairman FEINSTEIN. Can I stop you right there?

Mr. FINE. Sure.

Chairman FEINSTEIN. Supposing the passport was required to be machine-readable, tamper-resistant, and had certain biometric data included on it, with the numbers coming through, could all of that be handled in a timely way?

Mr. FINE. That would be a difficult issue. There are approximately 17 million visitors from visa waiver programs coming in each year.

Chairman FEINSTEIN. I understand it is 23 million.

Mr. FINE. My understanding is it was 17. It could be higher.

Chairman FEINSTEIN. Okay.

Mr. FINE. That would be a burden on the INS to do that. It would require sacrifices. It would require waiting, it would require longer lines. There are currently restrictions on the INS. They are required to clear planes in a certain period of time, 45 minutes. I don't think they could possibly do that with that kind of restriction on them.

Chairman FEINSTEIN. Is that an arbitrary restriction?

Mr. ZIGLAR. No, no. It is in the law.

Chairman FEINSTEIN. You have to clear a plane?

Mr. ZIGLAR. An international arrival has to be cleared by INS in 45 minutes under the law.

Chairman FEINSTEIN. Thank you. We could certainly change that.

[Laughter.]

Mr. ZIGLAR. And we appreciate that.

Chairman FEINSTEIN. Let me ask this question of INS. You are spending approximately $300 million a year on information systems. As I understand it, the Inspector General found that INS has spent $80 million on IDENT. The FBI has spent around $40 million for its new fingerprint system, which we understand is much better.

Perhaps, Senator Kyl, you would want to chime in right now on what you learned about the hold-up of the IDENT system.

Senator KYL. From the staff—and this would be directed to you, Commissioner Ziglar—our understanding is that the program was moved to full Justice last year to ensure that IAFIS and IDENT are married together before any more IDENT systems were put in place, which was consistent with what you said.

The note from staff says no one from Justice/INS has told the appropriators that the goals have been achieved, if they have been achieved. So it would be important to get something in writing to them about the status of this so that if they have been achieved, the moratorium can be eliminated. If you could get information regarding the status of that to the Congress—as you know, we are right in that time period right now, so that might be very helpful.

Mr. ZIGLAR. Senator Kyl, what I mentioned was that we are about to deploy the transitional work stations that will marry these two. So we would be glad to give you all the facts and figures on that.

The IDENT system, Madam Chairwoman, was deployed in, I believe, 1989 and we actually have 800 work stations out there. Over that period of time, we obviously had the development cost of it, we had the deployment costs, and then we have the O&M maintenance costs which have been running about $10 million a year, all in. So there is a longer-term investment horizon that is associated with IDENT than there is with respect to the IAFIS system.

By the way, just so people understand what the difference is, the IAFIS system is a ten-print system, as opposed to a two-print system. But the reliability of two fingerprints is very close to the reliability of ten fingerprints, if you will. The IAFIS system is designed for a somewhat different reason, and that is identifying criminal aliens, marrying it up with that, and prosecution. Our system is to identify who the person is and the reliability of it is very high.

Chairman FEINSTEIN. I don't want to run out of time.

Mr. ZIGLAR. Sure.

Chairman FEINSTEIN. Mr. Fine, let me ask you this question. You hear about all these systems. I mean, there is IAFIS, there is IDENT, there is ENFORCE. You can go right through it. None of them seem to talk to each other. They all seem to be different and none of them seem to put data in a central data bank from which all can call.

Is that correct, first of all? Secondly, would you take a look at what Senator Kyl just stated, whether it is, in fact, necessary to get something in writing to the appropriators to proceed with that system?

Mr. FINE. I would be happy to do that, Senator Feinstein. There are many systems. There are too many systems. Within the INS, there must be a hundred systems that don't talk to each other. Within the Government, there are many systems. There are some that do. The Interagency Border Information System does marry information from the State Department, from the FBI, from the INS. But that is a name-based system and that is one example of it.

It needs to happen more often and it needs to happen with biometric identifiers so that we are not relying on people's names. People use false names; people's names are similar. There has to be a greater coordination of effort in that regard.

With regard to IDENT, the problems with IDENT and IAFIS being married up started very early. These systems started in development in 1989. Both the FBI and the INS started their parallel systems, and the problem was that they both went their separate ways because they believed they needed different requirements.

So when the INS implemented its first IDENT system in 1994, the FBI was behind schedule. The FBI eventually brought it into fruition in 1989 without an adequate plan to have them married up, and that is the system we faced in 1999 and that is the system we still face today. They are developing plans. There are pilot studies going on, there are operational studies going on, but there is not an effective plan to bring them to fruition.

Chairman FEINSTEIN. What would you recommend?

Mr. FINE. I would recommend that they exert concerted effort on being able to decide what the operational requirements are, the funding needed, and implement that initially in a pilot project, but then move forward rapidly.

Chairman FEINSTEIN. Is there a need for everybody to have a different fingerprint mechanism? Can you not have one standard requirement for everybody with respect to fingerprints and then they go into a central base so that if something comes up and you need that instant communication between State, between INS, between FBI, and maybe even between CIA, you have got the ability to access it immediately?

Mr. FINE. I don't think there needs to be a separate standard for fingerprint systems. The problem is we have developed separate standards and now they need to be integrated, which is harder to do.

Chairman FEINSTEIN. My time is up.

Senator KYL. Take some more. I took some of yours.

Chairman FEINSTEIN. Let me just ask Ms. Ryan this question. Three of the 13 terrorists who received valid visas overstayed those visas but were not detected or removed from the United States.

What, in your view, went wrong in the issuance of valid visas that permitted these 13 terrorists to legally enter the United States, or do you view their entry as acceptable risk?

Ms. RYAN. What went wrong is that we had no information on them whatsoever from law enforcement or from intelligence, and so they came in, they applied for visas. They were interviewed and their stories were believed. I think, like most Americans, I was surprised at how much we learned about some of these terrorists in the immediate aftermath of the September 11 atrocities, and my

question in my own mind is why didn't we know that before September 11.

We were asked by the FBI to revoke visas on August 23rd of 2001, and we found that one person that they asked us to revoke we had no record of. Another had been refused. A third one, his visa had expired, and the fourth one obviously we revoked, but he was already in the United States.

We have had a struggle with the law enforcement and intelligence communities in getting information. We have tried in the Bureau of Consular Affairs my whole time in Consular Affairs to get access to NCIC III information from the FBI and we were constantly told we were not a law enforcement agency and so they couldn't give it to us. Other agencies fear compromise of sources and methods.

I really think that now that we have seen what people can do to us that we have to figure out how we can get this information that protects sources and methods, although I must say in the immediate aftermath of the plane crashes and the killings that the American people were told that a couple of these people had been at a meeting with Osama bin Laden operatives in January of the year 2000.

Mohammed Atta, who was alleged to be the ring-leader of this group, applied for and was issued a visa in May of 2000. Now, my question is when did we have this information as a Nation, as a Government. When did we know that he had met with Osama bin Laden operatives? And if it were known before we issued a visa, why didn't we know?

Chairman FEINSTEIN. How do you answer that yourself?

Ms. RYAN. I don't know, Madam Chairwoman. Either it is a colossal intelligence failure, in which case we had no information about them, and so that is what I would have to regard it as, a colossal intelligence failure, or there was information that was not shared with us who are the outer ring of border of security.

Chairman FEINSTEIN. But unless somewhere there is some common database, you might put restrictions on access to that common database and you might want to just limit it to the world of terrorism, but at least everybody would be feeding their information into a common database.

Ms. RYAN. Absolutely.

Chairman FEINSTEIN. If that were the case, then there could be a number of red lights that would go on with respect to certain people who present a hazard to the United States.

Ms. RYAN. Precisely.

Chairman FEINSTEIN. Absent this, it seems to me there is a piece in this agency, there is a piece in that agency, there is another piece in a third agency, and it never develops into a complete picture that can ring a bell and say, whoops, there is a problem here.

Ms. RYAN. I think after September 11 what we have seen is that just what you are describing must take place. I don't think there is any more turf business or any more worry about sources and methods. Information can be put into our system that exists right this minute, the system I described to you as a name check system, that can be put in in codes, the way the blind sheik was in the system but was not checked. Now, we have automated it, so it is im-

possible not to check—a double zero, which means you must refer the case to the visa office in Washington.

The visa office in Washington, of the Bureau of Consular Affairs in the State Department, then goes to the agency that put that person in and says this person has applied for a visa at this post. Do you want to admit them? Do you want us to refuse them? What do you want us to do with that case? That is what we need, Madam Chairwoman. That is what we have to get.

Chairman FEINSTEIN. I think that Ambassador Ryan has hit the nail on the head. I think, Senator Kyl, that that is what we need to strive for. Let me turn it over to you.

Senator KYL. Thank you. I agree. It is a cut-out system, it is known. We use it all the time.

I have got a couple of specific things which I will get out of the way, but then I think the overall question—and I think I want to address this primarily to you, Mr. Fine, at least first—we could easily get bogged down into the details. I mean, I have got so many questions here about the biometric border cards and all this kind of thing.

Frankly, with our five-minute questioning rounds and short attention span to this, and so on—and we lack the expertise—about the best thing we can do is to bring people together, shine some light on an issue, express a general policy direction and then turn to some people and say, now, please work this out, get something done, get recommendations to us with respect to any law changes or money that you need, and then we can move forward.

So I will let you think about my question for a minute. All three of you, of course, are welcome to respond, but with the new terrorism czar, Governor Ridge, taking office, maybe this is a place for this to be done.

It seems to me that a group needs to be convened of all of the relevant players, which would include all of the law enforcement and intelligence groups, the State Department, the INS with all of its different groups, Border Patrol, and Treasury with Customs, and the inspectors general of every one of these departments, and the Attorney General and others, and say, all right, we have a limited period of time to get everything coordinated and everything up to speed, how is this going to get done, and have a specific tasking group, a special group with that specific responsibility with respect to the issue that we are just talking about here today.

I mean, there are all kinds of issues that have to be dealt with, but this is a fairly discreet, although large, problem. I will recommend that to Governor Ridge, but I would like your response to that.

Just a couple of things back on this other issue. As you all know, the appropriators can be your friends. Here you have two right here. I think it is a matter of get information to them, don't wait for them to ask, don't wait to think about.

Again, from staff I have a note here that $27 million is in the bill this year for the integration of IDENT and IAFIS. And according to staff of Appropriations, this should "pretty well do it." Well, based upon what you said, Mr. Fine, maybe no amount of money can do it. I don't know. Is this right?

I think you need to get a report to them while the CJS bill is still extant and it hasn't been resolved yet, and sit down with them, in light of the new circumstances. I would say to the extent it is appropriate—I know there is a policy firewall here between the inspectors general and the departments, but you do make recommendations and if there is some way to break down a few of those barriers and get recommendations about how to deal with this specific problem and then figure out the money that you need, that is just one way to begin to think outside the box, as you yourself, Mr. Ziglar, have said we have got to do. This is a new era and we have just got to sit down and work these things out.

I was struck by your comment that 300 million non–U.S. citizens come into the United States every year. That obviously includes repeats of the same person, I presume.

Is that correct? Three hundred million non–U.S. citizens come into the United States every year?

Mr. ZIGLAR. It is actually more than that. It is probably closer to 350 million, Senator. I just said 300-plus because we have—

Senator KYL. And this is the legal entries.

Mr. ZIGLAR. These are people that come across our borders, yes, sir.

Senator KYL. Well, no.

Mr. ZIGLAR. Yes, yes.

Senator KYL. Okay, because we have another—

Mr. ZIGLAR. You have got to remember, Senator, only maybe half of the non–U.S. citizens that come here come on visas, or way less than half come on actual visas. Then they come under the visa waiver program, and then they have the exemption if they are Canadians, for example. So a lot of people come into this country that the State Department never sees.

Senator KYL. Right. Now, we have to make a couple of quick points. First of all, the vast, vast majority of those people come to this country and contribute to our country. We want them here. All of that goes without saying, but I am just going to say it because we are focusing here on part of the problem. It is also a limited part of the terrorist problem with respect to people who are here illegally.

But given the nature of this war that has been declared now, we can expect that this is going to be a significant component of fighting this war, making sure that we don't allow guests to come into this country who are going to cause us harm. So clearly we have a right to focus on these people, and I think that is the point I want to make.

With regard to this subcommittee's jurisdiction, clearly we have a huge technology challenge with respect to that. Now, with that in mind, and understanding that technology isn't the only way to fight this, but in one way or another we keep coming back to that, let me start with you, Mr. Fine.

If you were the President of the United States here and you had to figure out a way—and you are talking to Governor Ridge now and you are saying, Governor, I want you to get this part of the problem fixed. So what would you recommend we do so that we have got something in place here within the next 90 days, or whatever period of time, that we can get all of this information inte-

grated, the systems can be integrated, everything we need in terms of information gets in and we begin to operate in a more secure way? What would the recommendation be?

Mr. FINE. I agree with your recommendation. It is a problem that crosses agencies and it needs to be dealt with across agencies. And we need to bring together the knowledgeable people from the various agencies—the information technology people, the operational people, the policy people—and figure out a way to address this issue because it involves systems in the Justice Department, in the Treasury Department, in the State Department. We have too often dealt with these systems individually rather than in a coordinated fashion. So that does seem to be an area that Governor Ridge should and could deal with.

Chairman FEINSTEIN. Just one quick comment. Unless you have got the data from all of the agencies in one place, with some criteria for a potential terrorist definition to pop up, you are never going to be able to identify people who are potential threats. That is my concern in this, that we go on and we build a multiplicity of systems and they all fail dramatically because there isn't enough in any one system to identify a potential threat.

Senator Cantwell?

Senator CANTWELL. Thank you, Madam Chair. Again, thank you for your leadership on this issue and conducting these hearings.

Commissioner Ziglar, your enthusiasm in your new challenge has been noted, and your great relationship with the Hill. The challenge for us is going back over some of these problems that we have had before and I just wanted to make sure I understood some of your testimony.

The laser visa program that we have at our southern border which really was the first step in a biometric visa with, I believe, two-fingerprint information and a photograph—we haven't implemented that fully, because we are not using that system now at our southern borders because we don't have the readers.

Could you explain to me where we are on that program?

Mr. ZIGLAR. That is partly correct. The laser card is now in effect, and as of October 1 we were no longer accepting the old border crossing cards unless they had been—with respect to those people who been approved and hadn't actually received the card, we stamped it and clipped it, and they can use it until they get their new card.

That card has information about the folks in it. There have been 4 million of them, roughly, that have been approved for this and cards issued, thanks to Ambassador Ryan's operation. They did the approval. We actually did the production through of a contractor of the cards.

Senator CANTWELL. So somebody is actually crossing the border using this technology?

Mr. ZIGLAR. Yes, ma'am. The card has a photograph on it. What is not in place are the machine readers for these cards, and has been really an issue of money.

Senator CANTWELL. So we have a sophisticated card, but no technology, so an individual border agent or INS inspector is looking at this?

Mr. ZIGLAR. They look at the picture, but the fact is that these cards are pretty tamper-resistant and in a primary inspection mode that is what the cards would be used for. It is in a secondary mode that you would actually go and access the data and the biometrics of it. The machine readers for that have not been purchased and it has been a simple matter of not having the money appropriated.

The INS has in its budget requests since 1999 has asked for the money for this. Now, I am not blaming Congress. I have seen the budget submissions. They asked for it, the OMB cut them out, and they were never part of the President's budget coming up here. So the money has never been appropriated for it.

There is actually some good news in that. I know it sounds strange, but because of the advance in technology and because of the effectiveness, believe it or not, of the IDENT system, what we have in these little cards are the fingerprints of these folks that have applied for them. Those fingerprints have now been put into our IDENT system so that we can actually use a biometric through the IDENT system out of the process for using these cards, which means that we can now go to a more—I hate to use the word "generic" machine reader that can read lots of different kinds of biometric information out of different kinds of cards.

That is what we are proposing to do, is to buy a somewhat different machine than we would have employed earlier and integrate our IDENT system into the border crossing card system.

Senator CANTWELL. Is there a problem with IAFIS and IDENT on this in the sense that one is a two-fingerprint and the other is a ten-fingerprint role? Aren't there some integration issues?

Mr. ZIGLAR. That is a totally different issue.

Senator CANTWELL. But if we go down this one path with these two-fingerprint standards in one part of the system and then try to integrate it with another part of our information gathering—

Mr. ZIGLAR. No, it is really not. What we are trying to do is access the fingerprints that IAFIS has, and they will access the fingerprints that we have in IDENT. We have only two. They have ten, but the reliability of a two-print system is very, very high.

Notwithstanding what my friend the Inspector General said, the system is much further along. The Justice Management Division is actually honchoing the integration of this between the FBI and the INS, and we are going to be deploying transitional work stations that integrate the IAFIS and IDENT systems. The integration of IAFIS and IDENT does not in any way impede the effectiveness of the border crossing card or laser visa system at all.

Senator CANTWELL. Commissioner Ziglar, I want to get one more question in. We passed this legislation last night with authorizing language for tripling of border personnel—INS, Customs and border agents. Shouldn't we use some of the $10 billion that has already been appropriated by Congress to get started on that project so that we can meet the challenge that we have right now with increased security levels at our borders, the challenge of actually doing exit interviews at our borders, and the sheer lopsidedness of the number of people that are at our Canadian border?

Mr. ZIGLAR. Bless you for passing that and, yes, we should use some of that money.

Senator CANTWELL. Thank you.

Mr. ZIGLAR. By the way, just for your information—you will be interested, since you are on the northern border—the day before yesterday, I redeployed 100 Border Patrol agents that had been part of the contingent we sent to the airports around the country that are now being phased out because of the National Guard. I have redeployed them to the northern border.

We obviously have sent more inspectors up there. We now have 24/7 on all of our ports of entry on the border, in conjunction with the Customs Service. So we are moving rapidly and we have got some other ideas, some of them out of-the-box ideas about how we can upgrade our northern border security in a very short time frame.

Could I take one other second to say something? I couldn't endorse more what Mary Ryan just said about intelligence information being available. From a technological point of view, we can get access to this information in one place. That is not something that can't be done. We have the capacity to do that, but it doesn't matter how much capacity you have got if the information that you need in the system is not there.

What I saw before September 11 was a bunch of agencies with a bunch of territorial prerogatives that wouldn't share information. We didn't get NCIC III until fairly recently, and we only now have it at two of our ports of entry. Ambassador Ryan doesn't get it at all where she needs it.

Well, now, finally the Congress has mandated it, but we have to have Government agencies working together for the interests of the American people. And after September 11, I see something happening that should have happened a long time ago, and that is that we are working together, and that is very positive. We can solve the technology problems. We need the personnel, we need the money, but we can fix it.

Senator CANTWELL. Well, I know my time is expired, but using some of the $10 billion that has already been appropriated, as opposed to waiting until next January or February to address this issue and coming back to Congress on the second $10 billion that has yet to be detailed out, would be a very positive step.

Senator KYL. [Presiding.] Thank you very much. I will wait for the chairman to excuse this panel and call the next, though she had authorized me to do so, but I will express my personal thanks. I think we are probably going to quickly write a letter, probably to Governor Ridge, but we also will need to have you all be talking to the people you work with in support of this effort that we talked about here today.

Mr. ZIGLAR. Senator Kyl, if I could make one comment, don't get the idea that the executive branch isn't working in a coordinated fashion to do exactly what you are talking about. I am very involved in that. I haven't gotten much sleep in the last month, but I am going to tell you I am very involved in that. This administration, this executive branch—and this isn't partisan—is working very hard to try to bring together all of the things that you were talking about.

Chairman FEINSTEIN. [Presiding.] If I might, I would like to thank this panel and I would like to—you haven't asked your questions. I beg your pardon, Senator DeWine.

Senator DEWINE. You know, Madam Chairman, they were getting ready to leave. Mr. Ziglar was almost out the door.

[Laughter.]

Mr. ZIGLAR. I thought I had escaped, Senator.

Senator DEWINE. He thought he had escaped me, but he hasn't. Thank you very much.

Commissioner, what role has the INS played in the recent investigation after September 11, and how well have you all done? Give us just a quick summary.

Mr. ZIGLAR. We have played a very significant role, particularly with respect to the FBI. We have worked side by side with them both in the investigations and the interviews and the information-sharing. Notwithstanding the fact that we hadn't had really good information-sharing electronically speaking, if you will, we do now because there are plenty of ways that you can patch together systems that will make them work. They may not be as efficient as you would like them, but we clearly have done that.

We have generated an enormous number of leads independently of the FBI in this. I am not going to reveal numbers at this point, but I can tell you that this organization has responded magnificently to this.

Senator DEWINE. Well, good for you and good for your team.

Mr. ZIGLAR. It is not me; it is my team.

Senator DEWINE. Ambassador Ryan, whose job is it to see that all countries are complying with the visa waiver program, and are they? In other words, if we have somebody out of compliance, one of our partners, who is screaming about that?

Ms. RYAN. It is a joint responsibility that we share with the Department of Justice. In fact, the Commissioner and I met with our staffs immediately after September 11 to review the visa waiver program to take a look at countries that might be of more concern to us now after September 11.

We are going to have reassessment teams go out to six countries to discuss with them their passport controls and border patrols. We have pushed very hard. All the countries but one now issue machine-readable passports, the one being Switzerland, and they plan to introduce it in early 2003. But we have pushed very hard on all of those countries, and we look forward to working with the Department of Justice and the Immigration Service in going out to these countries, the six that are of concern to us, to discuss with them and perhaps to drop countries from this program.

Senator DEWINE. That was my next question. Do you have the authority to do that?

Ms. RYAN. After the reassessments are done, yes, sir.

Senator DEWINE. You don't need any permission from anybody? You can do that?

Mr. ZIGLAR. Well, we do it together.

Senator DEWINE. I understand, but you administratively do that?

Ms. RYAN. What we would do would be to make a recommendation to the Secretary of State and to the Attorney General that the Attorney General remove these countries from the program.

Senator DEWINE. Let me just say as one member of the United States Senate, please don't hesitate to do it if the facts are there.

Mr. ZIGLAR. We can and we will.

Senator DEWINE. If the facts are there.

Ms. RYAN. Exactly.

Senator DEWINE. We are through messing around.

Ms. RYAN. Indeed.

Senator DEWINE. All right. I think I can speak for most of my colleagues on that as well.

You mentioned the program on the visa fee and the ability to keep the visa fee. What are you able to keep on each visa?

Ms. RYAN. I can't thank you enough for what you have done for us. In the aftermath of the World Trade Center bombing, when the Congress recognized that we had a systemic problem—it wasn't a problem of a delinquent officer; it was a systemic problem that we were not automated—Congress gave us an authorization in fiscal year 1994 to charge a fee for every application for a non-immigrant visa and to keep the money.

That fee is now $45, and that is an application fee; that is not an issuance fee. Just about everybody who applies for a non-immigrant visa pays a $45 fee and we are able to keep that money. With that money, over the years since fiscal year 1994, we have automated the world.

Every visa-issuing post is online, in real-time, with the consular lookout system. It is a tremendous advance, a major advance in the protection of our borders, and it is because you all gave us that authorization and we were able to keep the money. Consular Services would have collapsed in the 1990s without that money.

I don't know if you have paid attention to what was happening to the State Department budget in the decade of the 1990s.

Senator DEWINE. Yes, I have.

Ms. RYAN. We were savaged. We are not even able to hire to attrition, let alone anything more than attrition. It was terrible. But with the money through the machine-readable visa fee which is paid for by aliens, by foreigners—not one cent of American taxpayer money has improved that system; it is paid for by the foreigners applying for visas—we are able to automate the world and to protect our Nation.

Senator DEWINE. Well, it is a good model.

Ms. RYAN. It is a tremendous, wonderful model.

Senator DEWINE. I think it makes a lot of sense and we ought to continue to look at different ways of doing that that do make sense.

One final comment and maybe a question to you, Mr. Ziglar. A lot of the theme of this hearing understandably has been on the integration of our systems and one part of the Government knowing what another part knows. It is an age-old problem. It is not unique to the INS. It is part of the way Government unfortunately operates, particularly in this country with all kinds of different agencies at the local, State and Federal level. I saw it as a county prosecutor and I have seen over the years in the law enforcement area at the local community level, having a judge in front of him or her and this person is a repeat offender and the data is not there and they don't know it. They have got a DWI in Indiana and we don't know it in Ohio, and it just goes on and on.

Ultimately, we can talk about it up here and we can have hearing after hearing, but you all are going to be the ones that have to fix it. I have looked at this for over 20 years and I think I know a lot about it, but there is an awful lot I don't know about it. I can't really get into the weeds and the other members of the panel can't get into the weeds. You have to fix it.

Our obligation, though, is, when you come to us, to give you the resources that you need. And my final comment would simply be—and as Senator Kyl has said, we have a few members of the Appropriations Committee here, and, Mr. Ziglar, you know an awful lot of people on the Hill—please don't hesitate to let us know what you all need. The climate is right to get it done. Let's get it done as fast as we can. God bless our friends at OMB, but I hope their priorities are set correctly this time.

Thank you.

Chairman FEINSTEIN. Let me thank the panel and let me just say that from my perspective, one overwhelming thing comes through. Thirteen out of 19 terrorists obtained valid visas. Clearly, our system is not able to prevent a terrorist from getting a visa legally to come into this country. That ought to be a sobering fact for all of us.

The more I listen to testimony, the more I come to the conclusion that we are never going to do it the way we are going, unless every agency of Government is able to enter into one terrorist-oriented database certain factors that they know about given individuals and that database is programmed to ring a bell when enough factors coincide, whatever the experts decide.

I am really concerned about continuing to appropriate money for systems that don't talk to each other. This is a colossal failure of our visa system. It doesn't keep out people who would come in and destroy us. So what else would you have a visa system for if not to do that? We might as well do away with it all and let everybody just come and go as they want to.

Ms. RYAN. I have to say that it is a failure of intelligence rather than a failure of the visa system. If we had the information, we would not have issued visas to these people. We did not have the information.

Chairman FEINSTEIN. Then that information on individuals has to go into that centralized system.

Ms. RYAN. Absolutely, but please don't say it is a failure of the visa system. I have visa officers all over the world who are devastated by the fact that they issued to these people. One of them told me you can tell me it is not my fault because we didn't have the information, but it is just as if a child ran in front of my car and I killed the child and everybody said it wasn't my fault; I have to live with that for the rest of my life.

So it isn't a failure of the visa system. It is a lack of information-sharing, a lack of intelligence. We have to fix that, Madam Chairwoman. We have to fix it.

Chairman FEINSTEIN. It is a failure of the system. You know, I hear one agency blame another and it is very upsetting to me. We don't have a system that works.

I would like to thank you all, and any ideas that you might have as to how the system can be made to work I think this sub-

committee would very much appreciate receiving. Thank you very much.

Mr. ZIGLAR. Thank you, Madam Chairman.

Mr. FINE. Thank you.

Chairman FEINSTEIN. I would like to welcome the witnesses of our second panel. They are going to be, after listening to the discussion, describing some of the potential technological solutions to the problems identified, I think, by the first panel.

We will begin with Mr. Steven Camarota. He is the Director of Research at the Center for Immigration Studies. He holds a master's degree in political science from the University of Pennsylvania and a Ph.D. in public policy analysis from the University of Virginia. He has testified before Congress on prior occasions and published widely on the political and economic effects of immigration. His articles on the impact have appeared in both academic publications and the popular press.

We are delighted to have him here today, and hopefully he is going to be able to shed some light on the vulnerabilities of our system and what might be done to correct them.

Mr. Camarota?

STATEMENT OF STEVEN A. CAMAROTA, DIRECTOR OF RESEARCH, CENTER FOR IMMIGRATION STUDIES, WASHINGTON, D.C.

Mr. CAMAROTA. Thank you very much. I would like to first, of course, thank the subcommittee for inviting me to testify today on an issue of critical importance to the future of our country.

As we consider our responses to the horrific attacks of September 11, we are clearly going to have to take action in many different areas. While it is absolutely essential that we not scapegoat immigrants or immigration, especially Muslim immigration, it is equally important that we recognize the most obvious fact: The current terrorist threat to the United States comes almost entirely from individuals who arrive from abroad. Thus, our immigration policy is critical to reducing the chance of future terrorist attacks.

There are a number of changes that seem obvious and that are clearly needed. To start with, we need a fundamental change in attitude. Unfortunately, some Americans have come to see our borders as simply an obstacle to be overcome by travelers and businesses. This attitude clearly has to change.

Most Americans certainly understand that our border is a critical tool for protecting our national interests. And by "border" I mean anyplace where foreign citizens enter the United States. A Zogby International poll taken in the—

Chairman FEINSTEIN. Mr. Camarota, let me interrupt you. I am going to ask them to strictly enforce the five-minute limit so that we can have some discussions among us.

Mr. CAMAROTA. Sure, okay.

Chairman FEINSTEIN. Thank you.

Mr. CAMAROTA. A Zogby International poll taken in the wake of the attack found that the overwhelming majority of Americans felt that lax screening of immigrants and border control contributed to the attack.

Now, in addition to a change in attitude, there are a number of practical things we can obviously do. First, there is visa processing overseas. Clearly, our consular staff of about 900 is extremely overworked, with 7.1 million non-immigrant visas or temporary visas being processed. The numbers are enormous and they are growing rapidly. Because of this ballooning of consular work, most consular officials only have a few minutes to interview each applicant. Clearly, more staff is needed.

Now, to successfully handle such a caseload and keep those out whom we need to keep out, the watch list, which is, of course, a compilation of names of people who are not to be issued visas, is our most important tool. To the extent possible, we need to integrate, as we have already heard, biometric measures in there. Many individuals who are on the watch list have already been arrested in their home countries or on prior stays in the United States, and to the extent possible we need to add fingerprints and photos to the list.

Of course, the next layer of defense is our borders. As we have heard, hundreds of millions of people cross our borders each year. Many more inspectors obviously need to be hired and we need more inspection stations. But most important, we need a system whereby all entries and exits are recorded to the United States.

The whole notion of a temporary visa is pointless if we don't know whether the time limit has been honored, and to do that we need an entry/exit system. Our visas should use smart card type technology containing a photo and fingerprints that can be scanned each time a person enters or exits the country.

Of course, these changes will be meaningless if it continues to be easy to cross the border illegally between crossing points. An inspector general report found that on the Canadian border, large sections of the border continue to be unmonitored.

Of course, again, technology can be very useful here. Not every inch of the border has to be manned. Advanced sensors designed to detect motion can be valuable force multipliers, but as we have already heard, they won't be very useful if there aren't enough of them and they don't cover the whole border and not enough agents are there to respond if one of them is triggered.

Of course, we also need to do something more in terms of interior enforcement. Current proposals for a tracking system for students must be extended to all non-student temporary visa-holders. Tracking is desirable because these long-term visitors reside here for long periods of time in legal status. Thus, they have time to hatch sophisticated plots.

While a tracking system is certainly important, the centerpiece of any interior enforcement strategy has to be in enforcing the prohibition on hiring illegal aliens. Worksite enforcement, as it is commonly called, is critically important for several reasons.

First, in terms of gaining control of the border, it will only be possible to do that if we reduce the number of people who are trying to come here looking for jobs. If they don't think the jobs are available, then they won't be crossing the border. Thus, it is critical to have worksite enforcement to gain control of the illegal crossing points of our border. Moreover, it will be much harder for terrorists

who overstay their visas to blend into the normal life of the United States if finding a job is made much more difficult.

Now, to have effective worksite enforcement, we need a national computerized system that allows employers to verify instantly that a person is legally entitled to work in the United States. Such a system would also have the advantage of letting us know where many legal immigrants, here on permanent residency visas, are working. At present, we have no idea where they are because they wouldn't be included in any temporary tracking system. So worksite enforcement could be a powerful tool for tracking people on permanent immigrant visas before they become citizens. Several terrorists in the past have been in that status, so this would be another important factor.

The last change that is needed is that we might need to consider, at least temporarily, a reduction in the number of permanent and temporary visas. The most important reason to do this is that the INS clearly needs time to have some breathing room to deal with the implementation of all the new technologies.

We are talking about increasing the size of its staff, and this kind of training and new investment requires a breathing space for the INS so that it can get up to speed. That is why I think we want to look at a reduction in the number of visas that we are issuing.

Some, of course, may object to a more tightly controlled border that uses the latest technology because it is looking for a needle in a haystack. But the point is all technology and all border enforcement and all kinds of security measures are always aimed at the tiny fraction of people who want to cross.

I see that I am out of time, so I will stop my comments now.

[The prepared statement of Mr. Camarota follows:]

STATEMENT OF STEVEN A. CAMAROTA, DIRECTOR OF RESEARCH CENTER FOR IMMIGRATION STUDIES, WASHINGTON, DC 20005

INTRODUCTION

The nation's responses to the horrific attacks of September 11 will clearly have to be in many different areas: including military retaliation, freezing terrorist assets, diplomatic initiatives, improvements in intelligence gathering, and expanded security measures at airports, utilities and other public places. But one aspect of increased preparedness must not be overlooked—changes in immigration and border control. Though alll the details have been released, it seems clear that the 19 terrorists of September 11 were all foreign citizens and entered the United States legally, as tourists, business travelers, or students. This was also true of the perpetrators of previous terrorist acts, including Ramzi Yousef, mastermind of the first World Trade Center bombing in 1993, Mir Amal Kasi, murderer of two CIA employees the same year, and Sheik Omar Abdel-Rahman, convicted in 1995 of plotting a terror campaign in New York.

While it is absolutely essential that we not scapegoat immigrants, especially Muslim immigrants, we also must not overlook the most obvious fact: the current terrorist threat to the United States comes almost exclusively from individuals who arrive from abroad. Thus, our immigration policy, including temporary and permanent visas issuance, border control, and efforts to deal with illegal immigration are all critical to reducing the chance of an attack in the future.

Much has been written about how we are involved in a new kind of war. In this new kind of conflict, America's borders are a major theater of operations. This is because the primary weapons of our enemies are not aircraft carriers or even commercial airliners, but rather the terrorists themselves—thus keeping the terrorists out or apprehending them after they get in is going to be an indispensible element of victory. The simple fact is that if the terrorists can't enter the country, they won't be able to commit an attack on American soil.

The president implicitly acknowledged this fact in announcing the creation of a new Office of Homeland Security, which "will lead, oversee and coordinate a comprehensive national strategy to safeguard our country against terrorism." In a very real sense, we already have a homeland security agency—it's called the Immigration and Naturalization Service (INS). The precursor of the INS was established in the Treasury Department in 1891 and moved to the new Department of Commerce and Labor in 1903. But in 1940, as war neared, it was moved to the Department of Justice. As Cornell professor Vernon Briggs has written, the move was done because "It was feared that immigration would become a way of entry for enemy spies and saboteurs," and President Roosevelt himself said the change was made solely for reasons of "national safety." A history of the INS describes its war-related duties: "Recording and fingerprinting every alien in the United States through the Alien Registration Program; . . . constant guard of national borders by the Border Patrol; record checks related to security clearances for immigrant defense workers. . ."

A Fundamental Change in Attitude About Our Nation's Borders

Most Americans understand that our border is a critical tool for protecting America's national interests. (By border I mean any place where foreign citizens enter the United States.) A Zogby International poll taken in the wake of the attacks found that the overwhelming majority of Americans, across all races, regions, incomes, and political beliefs blamed lax border control and screening of immigrants for contributing to the attacks and believed that improved immigration enforcement would reduce the likelihood of future atrocities.[1] There can be little doubt that greatly stepped-up efforts to control the border would be met with overwhelming support by the American people. Unfortunately a small but politically very influential portion of America's leadership has come to see our borders as simply an obstacle to be overcome by travelers and businesses. This attitude clearly has to change.

If we take the physical safety of our people seriously, our mechanisms for controlling and monitoring the movement of foreign citizens across our borders must be improved in three places: overseas, at the border itself, and inside the country.

Visa Processing Overseas

Entry to the United States is not a right, but a privilege, granted exclusively at our discretion. For the most part that discretion is exercised by members of the State Department's Bureau of Consular Affairs, often referred to as the Consular Corps. Among their other duties, these men and women make the all-important decisions about who gets a visa to enter the United States, making them the forward guard of homeland defense—America's other Border Patrol.

Recent improvements. Unfortunately, the Consular Corps has neither the manpower, nor the tools to fulfill this heavy responsibility properly. Most importantly, management of the consular corps offers distorted incentives to officers in the field. Mary Ryan, who became Assistant Secretary of State for Consular Affairs in 1993 and is in charge of visa issuance and the other consular responsibilities, has overseen genuine technical improvements in the issuing of visas. These changes have included making visas machine-readable and more difficult to forge than in the past. Also, the "watch list" of people who should not be granted visas is now computerized, rather than the old microfiche-based system in place until just a few years ago.

The American people and not visa applicants is the customer. But along with improvements, the Consular Corps has also adopted a culture of service rather than skepticism, in which visa officers are expected to consider their customers to be the visa applicants. Thus, satisfying the customer—the foreign visa applicant—has become one of the most important goals, leading to pressure to speed processing and approve marginal applications. As one former Foreign Service officer has written, "State Department procedures call for supervisory review of refusals, but not issuances—thus, relatively inexperienced junior officers are trusted to issue visas but are second-guessed on refusals."[2] Visa officers are judged by the number of interviews conducted each day and politeness to applicants rather than the thoroughness of screening applicants. This is especially ironic given that the law requires precisely the opposite approach, placing the burden of proof on the applicant for a temporary non-immigrant visa.

---

[1] The results of the Zogby International poll on immigration and terrorism can be found at www.cis.org/articles/2001/terrorpoll.html.

[2] Former State Department employee Nikolai Wenzel describes conditions at overseas consulates in a report public by the Center for Immigration Studies. The report is available at www.cis.org/articles/2000/back800.html

A Conflict of interest between visa processing and diplomacy. Responsibility for issuing visas fell to the State Department because it was the only agency with offices overseas, where the demand was. But it is difficult to imagine two less complementary functions than diplomacy and immigration enforcement. The diplomat's goal of promoting cooperation and compromise is sometimes in conflict with the gatekeeper's goal of exposing fraud and ensuring compliance with the law. This systemic mismatch is likely to persist regardless of management changes and may only be remedied by transferring all visa-issuing responsibilities overseas to the INS or perhaps a new "Visa Corps."

A new separate "Visa Corps?" A new free-standing visa issuing agency would have offices in consulates around the world, and would issue visas and be answerable not to the local ambassador, but to the head of this new agency or perhaps even the head of homeland security. If INS was to take control of visa processing overseas, then the Visa Corps could be answerable to INS headquarters in Washington. Moreover, if visa processing was the career choice of all visa officers, those who would work in this area would be able to hone their skills at spotting fraud or security risks. Visa officers need to be highly trained professionals, specializing in their function, respected by their agency, and insulated, to the extent possible, from political pressure. Such a system would be an invaluable asset in making our nations safer from terrorism.

More resources are needed. Administrative changes, of course, won't matter much if there aren't enough people to handle the work. The Bureau of Consular Affairs has only 900 Foreign Service officers overseas, assisted by 2,500 foreign nationals, and the demand for visas to visit the United States is enormous. Last year, the State Department issued 7.1 million non-immigrant visas, up 15 percent from 1995, and more than triple the number issued 30 years ago, when the majority of visas were issued to citizens of countries (mainly Western Europe and Japan) which now no longer need visas when arriving on short visits.

Because of this ballooning workload, all junior Foreign Service officers are required to adjudicate visa applications for a year or more, turning this profound responsibility into a dreaded rite of passage for new Foreign Service officers. Consular officers often have no more than a few minutes to assess each application. What's more, visa responsibilities are held in such low regard institutionally that consular ranks are often filled by unemployed spouses of local Foreign Service officers.

Watch lists and biometric identification. But even with adjusted incentives and adequate personnel, successfully handling such an enormous workload, and keeping out those who would do us harm requires the right tools. The primary tool in flagging terrorists is the "watch list," (also called the "look out" system) a compilation of several million people who are not to be issued visas. Obviously, effective intelligence is required for the watch list to be valuable, but based as it currently is solely on names, rather than also using a biometric identifier like a fingerprint, means that many possible terrorist might slip through. While fingerprints will never be available on most of those on the list, many persons on the watch list have been arrested or detained by authorities in other countries or on previous stays in the United States. To the extent possible we need to obtain these fingerprints and make them part of the watch list database.

To be most effective, the visa process should start with each applicant's fingerprints being digitally scanned into an integrated system which can be accessed by everyone involved in the immigration process—overseas, at the border, and within the country. These fingerprints should be checked against the watch list. Ideally, visitors' fingerprints should be scanned again when they enter the country, and again when they leave. This wouldn't be cheap to establish, but the technology is already widely used; in fact, the Border Patrol has been scanning fingerprints of illegal aliens apprehended on the Mexican border for several years now. Gathering applicant fingerprints and scanning them again when a person enters and leaves the country would serve many purposes: First, it would be a way of definitively determining that someone has entered the country and also that they have left when they are supposed to. Second: it would be a way of excluding those on the watch list for whom we have fingerprints. Third, it would establish identification, ensuring that the person issued the visa is the same person entering the country. Fourth, it would prevent individuals from going from consulate to consulate using different identities if they have been denied a visa at one location. Fifth, providing the U.S. government with fingerprints would by itself be a significant deterrent to would-be terrorists who certainly would be reluctant to give the government this information.

To the extent possible we also need to put photos of suspected terrorists on the watch list as well. If we took a digital photo of every visa applicant and ran it through facial recognition software, (which is already pretty well developed), along with fingerprints for each applicant, we might also be able to identify suspected

torrorists even if they apply for a visa using a false identity. While something like a facial recognition system would take time to implement, there are other simpler things we can do right away to make the list much more effective. the State Department's watch list could include access to the FBI criminal database, at present it does not. With the right management, staffing, and technology, the process of screening those we want to keep out would be much more effective. A number of procedural and legal changes would also help.

Exclude all enemies of America. Visa officers should be instructed to deny visas to people who are clearly enemies of America, but who have not actually committed a terrorist act. Currently, the law makes it extremely difficult to turn down an applicant because of his "beliefs, statements, or associations, if such beliefs, statements, or associations would be lawful within the United States." As the law now reads, keeping out a terrorist sympathizer, who publically organize demonstrations calling for the destruction of America or actively distributes Osama bin Laden videos, but who as far as we know, hasn't yet raised money for terrorist groups or planned out an assault, requires the Secretary of State to personally make the decision and then report each individual instance to congress. As a result, few if any individuals are excluded based on their anti-American beliefs.

We will not, of course, know the political beliefs of most applicants. However, just has we learn about the possible terrorist links of some individuals from friendly governments as well as our own intelligence, we will also learn of those who express strong anti-American views. These individuals can then be added to the watch list. Some may object to the idea of excluding people based only on their political beliefs, but it is important to remember that getting a visa to come to America is a privilege, not a right, and it is only common sense to exclude those who advocate violence towards our country. This is especially true during a time of war when the only way for the terrorist to attack us on our own soil is if we allow them into the country. Moreover, being denied a visa does not prevent such a person from continuing to express their views. He or she is free to do so in their own country. One can only imagine the American public's reaction if it is revealed in the aftermath of another attack that the anti-American views of the terrorist were know and he was still issued a visa to come to America. It is simply irresponsible not exclude all such individuals.

More through screening for applicants from some countries. Additionally, citizens of those countries whose governments do not sponsor terrorism, but whose citizens have come here as terrorists (Egypt or Saudi Arabia, for example) should have to pass a much higher bar for visa issuance, including a thorough security clearance (working with local authorities) and confirmation with universities of each student visa application. This should also apply to visa applicants born in these countries but now holding other citizenship. In addition, no visas should be issued to citizens of Middle Eastern countries at U.S. consulates outside their home countries; this is because an American visa officer in Germany is less likely to be able to identify a problem applicant from Saudi Arabia than his counterpart based in Saudi Arabia.

There is nothing unprecedented about such country-specific temporary visa policies; for instance, a person from Poland currently needs a visa to vacation in the United States, whereas a persons from Japan does not, because Poles are more likely to overstay their visas than Japanese. It is true that these provisions apply only to temporary visas, but a much higher bar for both temporary and permanent visas for nationals from some countries is simply a logical extension of this kind of policy.

Excluding persons based on religion or nationality is not justified. The fact that the terrorist attacks of September 11 were perpetrated by foreign-born Muslims may tempt some to support the elimination of visas for all Muslims or Middle Easterners in an effort to reduce or eliminate the foreign terrorist threat in the future. While more vigorous backgrounder checks for persons born in some countries makes sense and may result in a higher percentage being denied visas, efforts to exclude entire countries or religions should be resisted. Changes of this kind would harken back to immigration law prior to 1965 when the number of permanent residency visas were severely restricted for southern and eastern European countries, while immigration from Western Europe was much less restricted. Using religion or nationality as a basis for issuing visas is not only inconsistent with American values but may also anger Middle Eastern countries whose cooperation we very much need in the war on terrorism.

There may well be compelling national security or other reasons to reduce both temporary and permanent immigration, but changes should apply equally to all countries not just those in some parts of the world. Later in my testimony I explore some of the reasons why we may wish to reduce the overall level of immigration.

Selective enforcement of immigration law also must not be undertaken. For example, we should definitely not pursue visa overstayers who are from the Middle East

more vigorously than those from other counties. Instead, we need to develop enforcement strategies that apply forcefully to all overstayers. By definition all those who have overstayed their visas or entered the country without permission have broken the law and should be made to leave the country. Signaling out one group for enforcement is not only unfair and un-American but it is probably unconstitutional as well.

CONTROLLING THE BORDER

The next layer of protection is the border itself, which has two elements—"ports of entry," which are the points where people traveling by land, sea, or air entering the United States, and the stretches between those entry points. The first are staffed by immigration and Customs inspectors, the second monitored by the Border Patrol and the Coast Guard.

The need for improvements at the ports of entry is dire. Last year there were more than 500 million entries at these legal entry points, mostly at land border-crossings and many of them commuters. Close to half of these entries are returning U.S. citizens, and others are border commuters, but the number of foreign visitors is still enormous. In 1999, there were more than 31 million "non-immigrant" admissions (not counting Canadians and Mexicans on short visits), almost triple the number of 20 years ago. These were mostly tourists (24 million) and business travelers (4.5 million), but also included nearly a million students and exchange visitors and about the same number of "temporary" workers and corporate transferees. In fact, the INS states of the above numbers, "Inspections data for land passenger traffic are estimates that may contain unspecified margins of error." Put simply, the INS does not know how many people are entering the country.

A greater investment in manpower and infrastructure at the border. The land crossing points are often not fully staffed, and not every car or truck is examined. Part of the solution here is straightforward—many more inspectors and more inspection lanes at crossing points. Immigrant smuggling through ports of entry, using fake papers or hiding in secret compartments, was almost completely shut down when security along the borders was tightened in the wake of the September 11 attacks. The problem, of course, was that inadequate staffing and infrastructure caused long waits—but thorough checking plus additional inspectors can equal better security without excessive delay.

This attitude toward border security should have changed in December 1999, when one Ahmed Ressam was stopped by a border inspector at a crossing in Washington state. It turns out that he had trained at bin Laden's terrorist camps in Afghanistan and had a car full of explosives with which he was going to disrupt millennium celebrations in Seattle and blow up Los Angeles International Airport. He had entered Canada with a forged passport, requested political asylum, and was released into the population, pending a court date. This is standard practice in Canada, and underlines the importance of better border control.

Entry Exit System. There is also a long-standing and very real problem that the INS also does not know whether foreign visitors admitted on visas actually leave the country when their visas expire. There is no mechanism for tracking land departures, and the system for tracking arrivals and departures by air, which is how most visa-holders travel, is completely broken. The current system requires foreign visitors to fill out a two-part form with their name, passport number, destination. The visitor then hands one part to the U.S. immigration inspector upon arrival. The other half is collected by the flight attendants on the outbound flight and later transferred to the INS. The opportunities for failure are enormous: airlines often don't collect the forms or forward them to INS; visitors may enter by air but leave by land, leaving no trace of their departure; the information on the paper forms may be improperly keyed in. This system is so dysfunctional that the INS's own statistics division considers any departure data after 1992 to be worthless.

Time-limited visas are pointless with out entry-exit system. Temporary visa are only meaningful if we know whether the deadline has been honored. Because we do not collect accurate exit information, we have no way of knowing if someone has left the country. The result of this situation is a list of millions of people who appear not to have left, most of whom really have. Because of this, it is impossible to pick out the actual "visa over-stayers." As a result, if the FBI asks the INS if a particular individual is in the country, in may cases the INS must respond they simply do not know. In total, there are an estimated 3 to 4 million people living in the United States who entered the country legally, but never left, accounting for perhaps 40 percent of the total illegal-alien population.

The bipartisan U.S. Commission on Immigration Reform, headed by the late Barbara Jordan, in 1994 called for computerized tracking of all arrivals and departures

by land, sea, and air (including Canadians who don't need visas). Congress in the 1996 immigration law directed the INS to develop such a system, but partly at the behest of the business community in border-states, this provision was postponed and in 2000 effectively shelved. The concern was that the system would create interminable traffic jams as people lined up to enter and leave the United States—but a technologically modern system with an adequate number of scanners should not significantly impede traffic at all. This, of course, would mean greatly increased investment in equipment, personnel, and infrastructure at the border as well. For example, where there are now 10 lanes of traffic and inspection stations there may need to be 20 and where there are now 20 lanes there may need to be 40. The only other alternative is to expose the country to unacceptable risk.

Border Patrol is grossly inadequate. The situation isn't much better between the ports of entry. Better screening of visa applicants and a tightly monitored entry-exit system would be almost meaningless if it continues to be easy to cross the border illegally. A serious attempt has been made in recent years to increase the Border Patrol, although the total number of agents there is still only about 9,000 overall, and on any given shift, there are only about 1,700 agents on duty at the southern border or an average of less than one agent per mile. Moreover, there are only a few hundred agents patrolling the entire Canadian border, and this is where terrorists are more likely to enter for a variety of reasons, including the fact that immigrant communities in many Canadian cities provide excellent cover, whereas someone from the Middle East could not blend in so easily on the Mexican border.

A February 2000 report by the Justice Department's Inspector General sheds light on how inadequately the northern border is patrolled. It found that at one 300-mile sector of the border, agents identified 65 smuggling corridors but had only 36 sensors to monitor them.[3] Such sensors, designed to detect motion or heat or metallic objects, can be a valuable force-multiplier, but they will not be useful unless there are enough of them to cover the border and enough agents to respond when they are triggered. What's more, the IG report found that in some short-handed sectors, there are times when there are no agents on duty at all, a fact which quickly becomes apparent to various kinds of smugglers and terrorists trying to cross the border.

The answer, of course, is increased personnel and a serious commitment to border security. The Border Patrol has actually increased significantly since the mid-90s, and has been doing a much better job of patrolling the southern border, dramatically reducing illegal crossings near major cities and forcing smugglers to resort to more remote areas, where they are more easily detected. These successes need to be expanded upon while improving coverage of the northern border as well. The Border Patrol could be increased from its current total of less than 10,000 up to 30,000 or 40,000 people without even nearing the point of diminishing returns. This cannot be accomplished overnight, however, because it takes time to build a trained and experienced force. Nonetheless, failure to properly police the border between crossing points would be a huge invitation to terrorists rendering all our other efforts at immigration enforcement irrelevant.

Increased Border Patrol is not militarization. Some may object to such measures, and even to the increased border enforcement that has already taken place, as "militarization" of the border. Such objections highlight the important difference between the respective roles of soldiers and law enforcement; soldiers are supposed to find and kill the enemy, while law enforcement agencies, like the Border Patrol (and the Coast Guard), deter or apprehend wrongdoers. Assigning troops to patrol our borders would indeed be a militarization of border enforcement, and should be a very last resort (although using military support capabilities, such as radar and road-building, to assist the Border Patrol is appropriate, even necessary). But the way to avoid militarization is to build up the capacity of the Border Patrol such that there would be no reason to call for troops on the border.

INTERIOR ENFORCEMENT

The final layer of effective immigration control lies inside the country. As already discussed, the federal government has no idea whether foreign visitors have left when their visas expire. In addition, it has no idea where foreign citizens live when their visas are still valid.

Tracking tourists and business travelers would be difficult—even in the current environment, it is unrealistic to require all foreign visitors to submit their passports every time they check into a hotel and to expect hotels to report that information. Currently, foreign travelers are required to write down their destination upon enter-

[3] The entire report is available www.usdoj.gov./oig/i200004/i200004.htm.

ing the United States, but no effort is made to verify the information; in fact, two of the September 11 jihadists listed "Marriott Hotel, New York" as their destination. Resources could be more fruitfully spent elsewhere. Of course, this is why more stringent controls on issuing visas and real-time tracking of visa overstays are so important. But even with better screening and tracking of overstays, if we continue to almost entirely neglect enforcement of immigration law and allow millions of illegals to live in the country, we will also continue to expose our country to very significant terrorists threats. Fortunately there are a number of steps that can be taken to enforce the law within the United States.

A tracking system for temporary visa holders. Tracking of foreign citizens residing here for extended periods of time, affiliated with some American institution responsible for their whereabouts, is both possible and desirable. It's desirable because these long-term visitors (here from one to six years, or more) reside here for long periods of time in a legal status, whereas short-term visitors are less likely to have the time to hatch sophisticated plots before their visas expire. In our open society, there has been only the most perfunctory oversight of such long-term foreign students and workers—so perfunctory, in fact, that at least one of the September 11 terrorists entered the country on a student visa but never showed up for class, without triggering any concern anywhere.

And although short-term tourists and business travelers, who are not attached to any American institution, make up the majority of non-immigrants, the number of long-term visa holders requiring oversight is still quite large. In 1999, there were more than 923,000 foreign students and exchange visitors admitted (including their spouses and young children), up 45 percent just from 1995. The number of long-term foreign workers, plus family members, was about 1 million in 1999, up 123 percent from 1995.[4]

The 1996 immigration law mandated the INS to develop a computerized tracking system for foreign students, to replace the current manual, paper-based system. Unfortunately, the system has not gone beyond the pilot stage, and is only tested in a couple of dozen southeastern schools, largely because of opposition from universities and colleges. Institutions have opposed it, fearing the extra administrative burden associated with such a system. Many also do not like the idea of treating foreign students differently from their American counterparts. But given the very real threats we face, tracking all visitors makes perfect sense.

The problem with the whole foreign students program is not simply one of visa fraud or overstays; the nature of their studies is also a matter of concern. In 1997, the Washington Institute for Near East Policy published a report highlighting the weaknesses in our efforts to prevent students from terrorism-sponsoring states from studying subjects that would benefit those countries' weapons programs.[5] Not only are very few students denied visas based on their desired fields of study, but the lack of monitoring allows them to declare their intention to study some innocuous social science, for instance, but then change majors to nuclear engineering or the like, without anyone in the government being alerted to this fact.

Tracking system for foreign students must be expanded to non-students. The experimental INS system to track foreign students will almost certainly be accelerated in the wake of September 11. But this will not address the fact that there are an additional million temporary workers and trainees and intra-company transferees who are not included in the system, and they are not effectively tracked by any other means. Expanding the new tracking system to cover both foreign students and foreign workers is needed to ensure the system is as comprehensive as possible.

In a nutshell, to effectively control our border the government needs an integrated system that uses a biometric identifier like a fingerprint to create a single file for each foreign citizen planning to visit the United States, and track that person during the entire process—at each step in the visa process, each land border crossing, each entry and exit at airports, each change in status at school or work, each arrest, each application for government benefits. This file should be accessible to law enforcement and linked to the databases of the FBI, IRS, Social Security, Selective Service, and other federal agencies. There is no other way to keep admitting large numbers of foreign citizens and maintain security as well.

It is important to emphasize that at a time when there is much discussion of curbs on the civil liberties of Americans, better tracking of foreign citizens not only addresses the core of the security problem but should also be especially appealing because it does not effect the civil liberties of any Americans, only guests from overseas whose presence here is a privilege.

---

[4] Because the INS does not carefully track enter and exits, these figures include an unknown number of reentries by the same individual.

[5] A copy of the report can be found at the institute's web page www.washingtoninstitute.org

Ending Section 245(i) Another change regarding immigrants that would enhance homeland security would be the permanent elimination of a provision in the immigration law known as section "245(i)." This allows illegal aliens on the waiting list for a green card (because, for instance, they have married an American) to undergo visa processing and receive their permanent residence visa without having to leave the country and go to the U.S. consulate in their home country.

This provision is problematic not only because it rewards immigration line-jumpers but because it compromises homeland security. The INS official who processes the visa in the United States is much less likely to detect a possible terrorist or criminal among applicants than is a consular officer in the alien's home country, who is familiar with the local language and has contacts with local law enforcement. Not only does 245(i) undermine efforts to screen out terrorists, but it also negates our ability to keep out those judged to be dangerous—because they're already here, whereas an alien who went home only to be found ineligible would, in effect, have deported himself.

Enforcing the ban on hiring illegals aliens. The centerpiece of any interior enforcement strategy has to be enforcing the prohibition on hiring illegal aliens. While worksite enoforcement, as it is commonly called, may not seem to be vital to national security at first glance, it is in fact critically important to reducing the terrorist threat. In 1986, Congress prohibited the employment of illegal aliens, although enforcement was at first spotty and has been virtually non-existent for the past couple of years. Although it is obviously directed at turning off the magnet of jobs attracting conventional illegal aliens, such worksite enforcement is also important for anti-terrorism efforts. Gaining control of the border between crossing points is probably only possible if we dramatically reduce the number of illegal job seekers who routinely cross into the United States. If prospective illegal aliens knew there was no job waiting for them in the United States, many fewer would try and cross illegally.

In addition, it would be much harder for terrorists who overstay their visas to blend into normal life if finding a job is made much more difficult. Of course, they could still come with wads of cash and some might still live undetected, but doing so would be much harder to pull off if getting a job is much more difficult.

Even if one favors a guestworker program for workers from Mexico or elsewhere as the solution to illegal immigration, it would still be absolutely necessary to put in place a strong work site enforcement regime before implementing a guest worker program. Otherwise, there would be no incentive for those illegals already in the country or those thinking about entering illegally to sign up for such a program.

How would such a system work? There are two steps that are needed to make worksite enforcement effective. First, a national computerized system that allows employers to verify instantly that a person is legally entitled to work in the United States needs to be implemented. Employers would submit the name, date of birth, Social Security Number (SSN) or alien registration number to the INS of each new hire. Much of this information is already collected on paper, but is not used by the INS. After an instant check of its database, the employers would then receive back from the INS an authorization number indicating that the person is allowed to work in the United States. The authorization number from the INS would provide the employer with an iron-clad defense against the charge that they knowingly hired an illegal alien. Tests of such systems have generally been well received by employers.

Document fraud, of course, is widespread, but a computerized system would be a key tool in uncovering it. For example, a valid SSN that is attached to different names submitted to the INS or a SSN and name that show up in many different employers across the country would both be indications that a worker is trying to skirt the law. The INS could develop procedures to identify potential problems of this kind. When a potential problem is found, the INS would then go out to the employer and examine all the paperwork for the employee, perhaps conduct an interview with the worker and determine the source of the problem. This would require the second important change that is needed: a dramatic increase in the number of worksite inspectors. At present there are only the full-time equivalent of 300 INS inspectors devoted to worksite enforcement, whose job it is to enforce the ban on hiring the 5 or 6 million illegal immigrants now working in the country. These numbers would have to be increased to perhaps 3,000.

These inspectors would perform two main tasks: they would go out to employers identified by the verification system as having a potential problem and secondly they would randomly visit worksites to see that employers were filing the paperwork for each worker as required by law. Those employers found to be knowingly hiring illegals would be made to pay stiff fines. Because the data needed for such a system is already collected and the law already forbids the hiring of illegals, all that is need is a verification system and significantly more resources for worksite

inspectors. Failure to developed such a system means that millions of illegal immigrants will continue to work and live in the United State facing little or no penalty. Not only does this make a mockery of the rule of law, it also exposes the country to significant security risks.

Employment verification and alien registrations. Most of the recommendations outlined above have dealt with temporary visa holders or efforts to reduce illegal immigration. More effective monitoring is also needed of permanent residents, i.e., legal immigrants, with "green cards," who will after a time become eligible for citizenship. Several past terrorist attackers have been legal immigrants, and that may well increase as a result of military reprisals against terrorists overseas. In 1940, as a homeland security measure, Congress required all non-citizens living in the United States to register annually their whereabouts with the INS. This provision was repealed in the 1980s and should probably not be revived in that form. Potential terrorists cannot be expected to dutifully send in their addresses. However, the employment verification system outlined above could be a very effective tool in locating non-citizen legal immigrants. This is especially important when a person is placed on the watch list after he has entered the country. At present, there is often no way for the INS to know where that individual lives. However, the employment verification process would provide the INS with the employer for non-citizen legal immigrants who work. Thus, if it became necessary to arrest or at least undertake surveillance of a non-citizen, their last known employer would be a place to start. The verification system would in effect be alien registration for most resident aliens.

Integrated databases. One reform that would probably be relatively easy to undertake would be for the INS to integrate all of its various databases. At present, separate databases are maintained for non-immigrants, immigrants, citizenship applications, and deportations. The INS needs to establish a single integrated file on each foreign citizen that uses a biometric identifier like a digital fingerprint. This file would contain information from each step in the visa process: including each land border crossing, each entry and exit at airports, each change in status at school or work, each arrest, as well any application for permanent residence. This file should be accessible to law enforcement and would remain open until the person becomes a citizen.

REDUCE THE NUMBER OF PERMANENT AND TEMPORARY VISAS?

The responses outlined above, whether overseas, at the border, or inside the United States, would not catch all malefactors. But the improvements outlined above would almost certainly be very helpful in alerting us to large conspiracies like the September 11 attacks. If only a few of the dozens of conspirators had been identified by consular officers or border inspectors, it is very likely that the entire conspiracy would have unraveled.

Less immigration means better enforcement. But what of the actual number of people we admit via these mechanisms? There are two fundamental reasons to consider reducing the number of student, exchange and worker temporary visas, and permanent residence visas: the fewer visas we issue the more thorough the background checks that can be conducted. Moreover, fewer visas also mean fewer foreign nationals living in the United States, making it much easier to keep track of those allowed into the country.

It seems very unlikely that the INS and State Department can undertake the necessary reforms and expansions if they also have to continue processing hundreds of thousands of new immigrant, foreign student, exchange and worker visas each year. The General Accounting Office reported in May that the receipt of new applications (green cards, citizenship, temporary workers, etc.) has increased 50 percent over the past six years, while the backlog of unresolved applications has quadrupled to nearly 4 million. Few if any government agencies could be expected to handle such a crush of new work while assuming added responsibilities, even if provided with increased resources. The INS in particular has had a great deal of difficulty in modernizing and using additional resources. Its computer systems, for example, are among the most outdated in any part of the federal government. This stems from a decision in the 1970s not to automate the files so as to preserve low-level clerical jobs. As then-Commissioner Doris Meissner told Government Executive magazine in a 1999 interview, "You don't overcome a history like that in four to five years."

Solving the many problems with our immigration system will not be easy. There have been various plans to reorganize the INS altogether, including splitting the service and enforcement functions, either into two agencies or two separate chains of command within the current INS. But money and institutional reorganization won't be enough on their own. The best way to give the INS the breathing room

it needs to put its house in order and to address homeland security concerns is to reduce its workload by reducing temporary and permanent immigration.

CONCLUSION

The fundamental changes in our immigration system proposed above should be an especially attractive option because not only would they be politically popular, but they also would not involve any infringement on the civil rights of American citizens. The American people are going to have to wait in much longer lines at airports and in other public places from now on, it is not too much to ask foreign citizens to do the same.

Some may object to greatly increased screening, interior enforcement and border control because only an tiny fraction of the millions of immigrants and visitors (or non-immigrants) who come to the United States each year represent a security threat. We are, some would say, looking for "a needle in a hay stack" by focusing on immigration reforms. But this objection makes little sense. All security measures are directed at only the tiny fraction of the population who wish to break the law. Every persons who boards an airplane, for example, must pass through a metal detector and have his baggage x-rayed. This is done not because most or many intend to hijack the plane, but rather for the one out of a million who is planning to do so. It is the same with screening immigrants and controlling the border.

To be sure, no steps to reform immigration will catch all those who mean us harm. But a lower level of immigration and dramatic improvements in visa processing and border security could make an enormous difference. If only a few of the dozens of people involved in the September 11 plot had been identified by consular officers or border inspectors, or been apprehended when their visas expire it is very possible that the entire conspiracy would have been uncovered. Persistent terrorists will, of course, continue to probe our immigration system for weaknesses. It is for this reason that we cannot, for example, improve visa processing but leave large sections of our land border undefended. Only a vigorous, well-funded, integrated border management infrastructure which employs the latest technology and enjoys sustained political support can be expected to adapt to the every changing terrorist threat. Moreover, only a well funded and run immigration system will be able to utilize the new information that is expected to result from the added resources that are now being devoted to intelligence gathering. Today's underfunded and fragmented border control system, using out-of-date technology, will certainly not be able to respond to the shifting challenges of the future.

There can be little question that the suggested changes outlined above would cost taxpayers billions of dollars to implement. But the alternative is to expose the country to very significant risks that could be avoided. If we want the American people to continue to support legal immigration, then we must make every effort to reduce the possibility of terrorism in the future.

Chairman FEINSTEIN. Thanks very much, Mr. Camarota.

We will now turn to David Ward, the President of the American Council on Education. He has served for 8 years as the 25th Chancellor of the University of Wisconsin. He was born in Great Britain, and he will testify on the responsibilities of American schools and universities to keep track of students from other countries.

Mr. Ward, welcome.

STATEMENT OF DAVID WARD, PRESIDENT, AMERICAN COUNCIL ON EDUCATION, WASHINGTON, D.C.

Mr. WARD. Thank you, Madam Chairman and members of the subcommittee.

ACE represents 1,800 public and private colleges and universities. And in addition to that organization, of which I am the president, I am speaking on behalf of many other higher education associations and the more than 6,800 institutions of higher education and the 15 million students we represent.

I am also accompanied by Mr. Ted Goode, Director of Services for International Students and Scholars at the University of California at Berkeley and an expert in the trenches on the complex process

by which international students are admitted to the United States, a matter in which I have a kind of personal interest.

I first came to the United States on a student visa in 1960 to attend the University of Wisconsin. I was interviewed for 15 minutes by the consulate in London. When I arrived here, I registered my address and my program every January 1, and when I completed my Ph.D. in 1963, the university reported that fact and I received a note that it would be useful for me to leave in one month, which I did. I later returned as an emigrant because I enjoyed that experience and I, in fact, became a Bicentennial citizen in 1976.

I strongly believe that our Nation as a whole benefits from having international students on our campuses, but I also understand that the opportunity to study in our Nation comes with rules and responsibilities that affect both students and our institutions. American colleges and universities have to understand this, and we certainly accept our role wholeheartedly.

Let there be no doubt of our position. The Federal Government has the right and the responsibility to protect the safety and security of the United States by deciding who should receive a student or exchange visa. Colleges and universities have an obligation and a responsibility to work cooperatively with the Federal Government in admitting students to this country and keeping track of them when they are enrolled on our campuses.

We believe the single most important step in improving our ability to monitor international students and work with Federal authorities will come from the prompt implementation of CIPRIS, now known as SEVIS, the Student and Exchange Visitor Information System. SEVIS has an important mission. However, it has long suffered from an exceptionally complex funding and administrative structure that has delayed its development and deployment.

Indeed, INS' efforts with respect to this system have created a great deal of apprehension and mistrust about the agency's ability to establish an electronic system without seriously compromising the ability of our colleges and universities to attract international students in competition with other nations.

Because of our reservations about the fee collection system, we strongly support your proposal, Madam Chair, to authorize an appropriation to cover the costs of developing this database. We believe that such a step will accelerate implementation. We appreciate the fact that you have sent a letter to the President asking that he allocate funding from the emergency supplemental appropriations package to speed the development and implementation of this system, and we have also sent a letter to the President endorsing your suggestion.

I would like to, however, make three additional points with respect to SEVIS. First, we believe that the implementation of the system will require that INS establish a clear timetable with interim goals. Because of the delays that have plagued the system from the beginning, we believe Congress should insist that INS specify the deadlines it will meet so that our institutions can also in a parallel way be responsive.

Second, INS has not yet provided us with adequate information about the computer system capabilities that will be required to implement SEVIS on campuses. This information is essential for in-

stitutions that need to reassess their computer systems' and data systems' capabilities in the light of these new responsibilities.

Chairman FEINSTEIN. If you will allow me to interrupt you, explain a little bit more about what you need to do it.

Mr. WARD. Well, it would be the software to connect our personnel data systems with those the INS has, and that will probably be a private sector development and we don't know what those specifications are yet. If this implementation is going on, we would like full notice of that so we can give specifications to vendors to develop the data system connection. The data system connection is the challenge.

We have gone through a revolution in higher education in personnel systems in the 1990s. We have our data. We need to get the data to INS, so we need to have a schedule and specifications.

Chairman FEINSTEIN. Thank you.

Mr. WARD. We can therefore speed implementation, but we do require reciprocity from INS, and I am sure we will get that on the basis of this morning's testimony.

Third, we believe it is essential to provide a modest appropriation to cover annual operating costs when the system is in place. This will eliminate the fee collection problems which are quite serious—about where to collect them, who should collect them, whether it should be the Department of Justice, the universities, the Immigration Service. It is a great challenge, and that really has been the problem with CIPRIS to date.

We also understand something else, Madam Chairman, which we have not really thought enough about—and we value your contribution to our debate over the last week—and that is your concern that potential international students may receive more than one I–20 form if they apply to or are admitted by multiple colleges in the United States. Just like your children and grandchildren, you never apply to one college. There are always multiple applications, and therefore there are multiple I–20 forms.

I have brought a chart which thinks outside of the box. It suggests a change in the way the whole I–20 system could be developed. We believe, in fact, that the only way to ensure that potential students do not get more than one I–20 is to avoid giving them the I–20 in the first place.

Therefore, rather than sending an I–20 directly to the student, as is done at present from the university to the student, we strongly recommend that the colleges send the I–20 form directly to a U.S. embassy or consulate identified by the potential student. This approach will also provide an easy way to ensure that students who receive a visa to study at a particular institution actually enroll there.

We recommend that each American embassy or consulate be asked to identify a student and exchange visitor visa coordinator. The name and address and information for this person should be posted on the State Department Web page to permit schools with questions about specific visas to be able to contact the appropriate person directly, should there be a problem.

My colleagues and I look forward to discussing these ideas with you in more detail in the very near future.

Madam Chair, you come from the State with the greatest number of international students and you know firsthand the benefits of international education. In California alone, 66,300 students were enrolled from abroad in 1999–2000. The overwhelming majority will leave as fans of California, or maybe USC, or even, heaven forbid, Stanford—true friends of the United States, leaders of government and industry in their home countries, and supporters of the benefits of personal freedom and democracy.

I believe that the proposals in the legislation you have prepared and the ideas I have laid out today to address your concerns about the I–20 form will, in both the short and the long term, be important steps in this direction.

I appreciate the opportunity to be here with you today and I would be happy to answer any questions at the appropriate moment.

[The prepared statement of Mr. Ward follows:]

STATEMENT OF DR. DAVID WARD, PRESIDENT, AMERICAN COUNCIL ON EDUCATION, WASHINGTON, D.C.

My name is David Ward and I am President of the American Council on Education (ACE), an association representing 1,800 public and private colleges and universities. I am speaking today on behalf of nearly 50 higher education associations and the more than 6,800 institutions of higher education and 15 million students we represent.

I am accompanied by Mr. Ted Goode, the Director for International Students and Scholars at the University of California, Berkeley, and an expert in the complex process by which international students are admitted to U.S. colleges and receive visas to study here.

The recent terrorist attacks on the United States have prompted a top to bottom review of all sorts of government and institutional activities. This reassessment includes questions about the international students who come to this country on a student visa to study at our colleges and universities. At present, it appears that none of those directly involved in the terrorist attacks entered the United States on a student visa. However, this does not obviate the need for a careful review of the policies and procedures affecting student visas. Madam Chair, we appreciate the chance to participate in this review and thank you for your leadership in this area.

I am-particularly interested in this issue for professional and personal reasons. Before assuming the presidency of the American Council on Education a month ago, I was Chancellor of the University of Wisconsin, Madison, for eight years, where I was a faculty member for 25 years prior to that. As one of the nation's leading research universities, UW Madison always had a large number of foreign students on campus, often more than 4,000. Without exception, I found them to be diligent and hardworking individuals who contributed significantly to the academic and social life of the campus.

I also have a deeply personal interest in this issue. I first came to the United States on a student visa in 1960 to earn a Ph.D. in geography at Wisconsin. At the conclusion of my Ph.D. program, I was given thirty days to leave the country in accordance with the terms of my visa. After living abroad for three years, I returned to the United States as an immigrant and became a citizen in 1976.

These experiences have given me a fairly unique position to appreciate the benefits that accrue to international students, American students, and the university community when we invite foreign students to study at our colleges.

The nation as a whole also benefits from having international students study on our campuses. For example, the enormous advances in computational sciences in the 1980s that helped fuel the American economy in the 1990s, would not have occurred without student and faculty exchange programs that brought so many talented people to this county.

We deeply appreciate the strong expression of support shown by the Senate in recently passing S. Con. Res. 7, which advocates the establishment of an international education policy to further our national security, foreign policy, and economic competitiveness. We hope the House will soon pass this measure. Now, more than ever, Congressional leadership is essential in ensuring that we equip the best and the

brightest—from our own nation and from abroad—to meet the challenges of an increasingly complex—and may I say more dangerous—world.

In this spirit, we understand that the opportunity to study in our nation comes with rules and responsibilities that affect both students and institutions. American colleges and universities understand this and accept our role wholeheartedly.

Let there be no doubt of our position: the federal government has the right and the responsibility to protect the safety and security of the United States by deciding who should receive a student or exchange visa. Colleges and universities have an obligation and a responsibility to work cooperatively with the federal government in keeping track of international students when they are enrolled on our campuses.

I assure you that we take this responsibility very seriously. Any college or university with significant numbers of foreign students maintains an international students' office and devotes considerable resources to continual in-service training in order to keep staff responsible for foreign students up to date on the large and constantly expanding body of regulation that governs this area.

On the Wisconsin, Madison, campus alone, over 20 full time employees are devoted to monitoring international student visa documentation issues. Nationwide, more than 3,000 higher education administrators have primary responsibility for foreign students on our campuses.

Our shared responsibilities are not in conflict and the relationship between the colleges and the government is generally constructive and collaborative. At present, colleges are required to maintain more than a dozen types of information on each international student and to make that information available to federal authorities upon request. The question before this committee is how our relationship can be made more proactive and how can we increase our emphasis on safeguards.

We believe that the single most important step in improving our ability to monitor international students and work with federal authorities will come from the prompt implementation of the Coordinated Interagency Partnership Regulating International Students (CIPRIS), now known as the Student and Exchange Visitor Information System (SEVIS).

As you well know, this is an electronic tracking system that will enable colleges to notify the Immigration and Naturalization Service (INS) whenever there is a "change of status" that may affect a student's visa. Under the law, when SEVIS is fully operational, the INS will be notified of: the identity and current address of all foreign students enrolled at our institutions; their nonimmigrant classification and any change therein; the date their visa was issued or extended; their current academic status, including whether they are maintaining status as a full-time student; and any disciplinary action taken by the school as a result of their having been convicted of a crime.

Because it is an electronic system, this information will be transmitted to federal officials for appropriate action almost immediately. SEVIS will stand in stark contrast to the obsolete paper and pencil system that is currently in use.

SEVIS has an important mission. However, it has long suffered from an exceptionally complex funding and administrative structure that has significantly delayed its development and deployment. Indeed, the INSs efforts with respect to this system have created a great deal of apprehension and mistrust on campus about the agency's ability to establish an electronic system without seriously compromising the ability of American colleges to serve international students.

Unfortunately, Commissioner Ziglar testified on October 3'd and again on October 11' that that the "academic establishment" is responsible for the delay in SEVIS's development and deployment. This is not true. This system has been over budget and behind schedule since it was begun in 1995. However, the history of SEVIS is not what we are here to discuss today.

Let me be clear. The American Council on Education has never opposed the underlying idea behind SEVIS—an electronic exchange of information about international students to facilitate monitoring and tracking. As I noted above, we strongly believe that the federal government has the right and responsibility to do this and colleges have an obligation to help provide this information. However, we have consistently and strongly opposed the INSs efforts to implement the fee collection system that is designed to cover the cost of developing SEVIS. The first INS proposal would have turned colleges into bill collectors for the federal government and we vigorously opposed that plan. Eventually, Congress blocked the INS from moving in that direction.

The INS is now considering another approach that we believe would seriously undermine the ability of most foreign students to enroll at American colleges. The new plan would require that students pay the fee using the Internet and a credit card or in American dollars before obtaining a visa. Many international students do not

have access to credit cards, American dollars, or the Internet. We believe that this proposal is worse than the initial plan that Congress blocked.

We strongly support your proposal to authorize an appropriation to cover the costs of developing this database. This step will result in much faster implementation than would otherwise be the case. We appreciate that you have asked the President to allocate funding from the Emergency Supplemental appropriations package (P.L. 10738) to speed the development and implementation of this system. We have sent the President a letter endorsing your suggestion.

I would make three additional points with respect to SEVIS. First, the timely implementation of SEVIS will require that the INS establish a clear timetable with interim goals so that Congress and the education community can measure the agency's progress against its own timetable. Based on our experience to date and the delays that have plagued this system from the beginning, we would ask that Congress insist on accountability in meeting this critical deadline.

Second, despite repeated requests, INS has not provided us with adequate information about the computer system capabilities that will be required to implement SEVIS on campuses. This information is essential for the private sector vendors who will develop and sell the software and for institutions that need to reassess their system capabilities in light of the new responsibilities. Within a week, we will share a detailed list of questions about the computer systems necessary to implement SEVIS and we would greatly appreciate your assistance in getting answers to these questions. Again, we will do all we can to speed implementation, but we require reciprocity from INS to make that happen.

Third, in addition to funding the development of SEVIS as your legislation provides, we believe it absolutely essential that a modest authorization be available to cover the annual operating costs when the system is in place. As I noted earlier, the primary barrier to acceptance of SEVIS has been the inability of INS to devise a workable method of financing the system. Because neither the State Department nor the INS has been willing to collect the money, the INS has been forced to develop terribly convoluted payment systems. I strongly urge you to add language to your legislation that will provide the modest amount of money needed to operate SEVIS when it is operational.

We believe that SEVIS is ultimately the only way to obtain the information that the federal government wants and needs. However, since this system will not be operational for several years, we believe that several additional steps could be taken to improve the government's oversight of student visas in the interim. We have already shared these ideas with your office and I have appended a copy of them to this testimony. (See Appendices One and Two.)

In some cases, we propose that new responsibilities be given to institutions of higher education. In other cases, we believe that the INS should be given additional assignments. Moreover, we believe that it is desirable to provide special scrutiny for potential students from countries on the State Department's watch list of states supporting terrorism.

Finally, we strongly recommend that the federal government increase funding for Department of State consular affairs offices to enable a more extensive review of student and all other visa applicants. These civil servants are the individuals responsible for making decisions about whether or not to grant a visa and we feel strongly that these offices ought to have the resources to accomplish their mission. At present, most of them do not.

We understand your concern about the possibility that potential international students may receive more than one I–20 form if they apply to and are admitted by multiple colleges in the United States. The multiple I–20s can be used to obtain more than one visa.

To address this problem, we propose that colleges send the I–20 form directly to a U.S. embassy or consulate identified by the potential student rather than the current practice of sending an I–20 directly to the student. We believe that the only way to ensure that potential students do not get more than one I–20 is to avoid giving them any I–20s in the first place. In addition, this approach will provide an easy way to ensure that students who receive a visa to study at a particular institution actually enroll there.

Under our plan, an institution of higher education would provide an I–20 for every international student admitted to an embassy or consulate, identified by the student. As under current practice, a potential student would go to the appropriate embassy or consulate to receive a visa and a visa would only be issued if a valid I–20 were on hand. If a visa were awarded, the embassy or consulate would return a copy of the I–20 to the sending institution to alert the college to expect the student. Such a step would provide an additional mechanism to help schools and the INS identify the small number of students who receive a visa but who fail to enroll.

We recommend that each American embassy or consulate be asked to identify a "Student and Exchange Visitor Visa Coordinator." The name and address information for this person should be posted on the State Department Web page to permit schools with questions about specific visas to contact the appropriate person directly.

My colleagues and I look forward to discussing this idea with you in more detail in the near future.

Madam Chair, you come from the state with the greatest number of international students and you know first hand the benefits of international education. In California alone, 66,305 students were enrolled from abroad in 1999-2000 and they brought $1.6 billion dollars into the state's economy. The overwhelming majority will leave as fans of California and as true friends of the United States.

Over the last 50 years, efforts to enable foreign students to study on our campuses have paid great dividends for our nation. Most will leave the U.S. at the conclusion of their studies and will become leaders in government and industry in their home countries. However, all of those who study here will leave with a deep appreciation of the benefits of personal freedom and democracy.

Education increases familiarity and understanding. Familiarity and understanding are incompatible with terrorism. Indeed, if we wish to increase international understanding, we ought to increase the opportunities for students from other countries to study in the United States. Important as this goal may be however, the most important assignment of the federal government and higher education is to ensure that students who come here to study pose absolutely no threat to American safety and security. I believe that the proposals in the legislation you have prepared and the ideas I have laid out today will—in both the short and long term—be important steps in this direction.

On behalf of:

Alliance for International Educational and Cultural Exchange
American Association of Colleges of Nursing
American Association of Collegiate Registrars and Admissions Officers
American Association of Community Colleges
American Association of Presidents of Independent Colleges and Universities
American Association of State Colleges and Universities
American Council on Education
American Dental Education Association
American Society for Engineering Education
Associated Colleges of the Midwest
Association of American Colleges and Universities
Association of American Medical Colleges
Association of American Universities
Association of Chiropractic Colleges
Association of Community College Trustees
Association of Governing Boards
Association of Independent California Colleges and Universities
Association of Independent Colleges of Art and Design
Association of International Education Administrators
Association of Jesuit Colleges and Universities
Association of Proprietary Colleges
California Community Colleges
California State University System
Career College Association
Coalition of Higher Education Assistance Organizations
Consortium of Universities of the Washington Metropolitan Area
Council for Advancement and Support of Education
Council for Christian Colleges & Universities
Council for Higher Education Accreditation
Council for Higher Education of the United Church of Christ
Council of Graduate Schools
Council of Independent Colleges
Hispanic Association of Colleges and Universities
Lutheran Educational Conference of North America
NAFSA: Association of International Educators
National Association of College and University Business Officers
National Association of Graduate-Professional Students
National Association of Independent Colleges and Universities
National Association of State Universities and Land-Grant Colleges
National Association of Student Financial Aid Administrators

National Association of Student Personnel Administrators
The College Board
University Continuing Education Association
University of California System

APPENDIX 1

HIGHER EDUCATION'S PROPOSALS FOR IMPROVING THE ISSUANCE AND TRACKING OF FOREIGN STUDENT VISAS

New Responsibilities for Institutions

Within 30 days of the end of the enrollment period at the start of each academic term, supply an electronic update to INS of the most recent data on enrolled international students covering the following items: date of commencement of studies; degree program and field of study; termination date and reason; and status (i.e. full-time or part-time).

Require higher education institutions to report to the INS within 30 days of the start of an academic term the non-appearance of any such student indicated by the INS to have entered the country on that institution's I–20 form or who accepted an offer of admission but did not enroll.

Require designated school officials (DSOs) to comply with any "revised responsibilities" outlined by INS or lose authority to issue I–20s.

New Responsibilities for INS

Notify a higher education institution within 15 days of a foreign student's entry into the United States using that institution's form I–20.

Issue a "revised statement of responsibilities" for DSOs that takes into account new reporting requirements.

Funding and Oversight

Guarantee the rapid implementation and effective operation of the Student and Exchange Visitor Information System (SEVIS) by replacing the current fee system with a permanent authorization and necessary appropriations.

Increase the budget for consular affairs at the Department of State to provide additional staffing, improve facilities where necessary, and mandate more effective use of information technology.

Provide sufficient funding for the expeditious implementation of an electronic arrival/ departure system for all visa classifications, as mandated by Section 110 of IIRAIRA.

Provide clarification that data disclosures to the INS regarding foreign students are not subject to restrictions under the Family Education Rights and Privacy Act.

Special scrutiny for limited categories of applicants.

Require consular officials to conduct more extensive background checks on student visa applicants from countries on the State Department's watch list of states supporting terrorism.

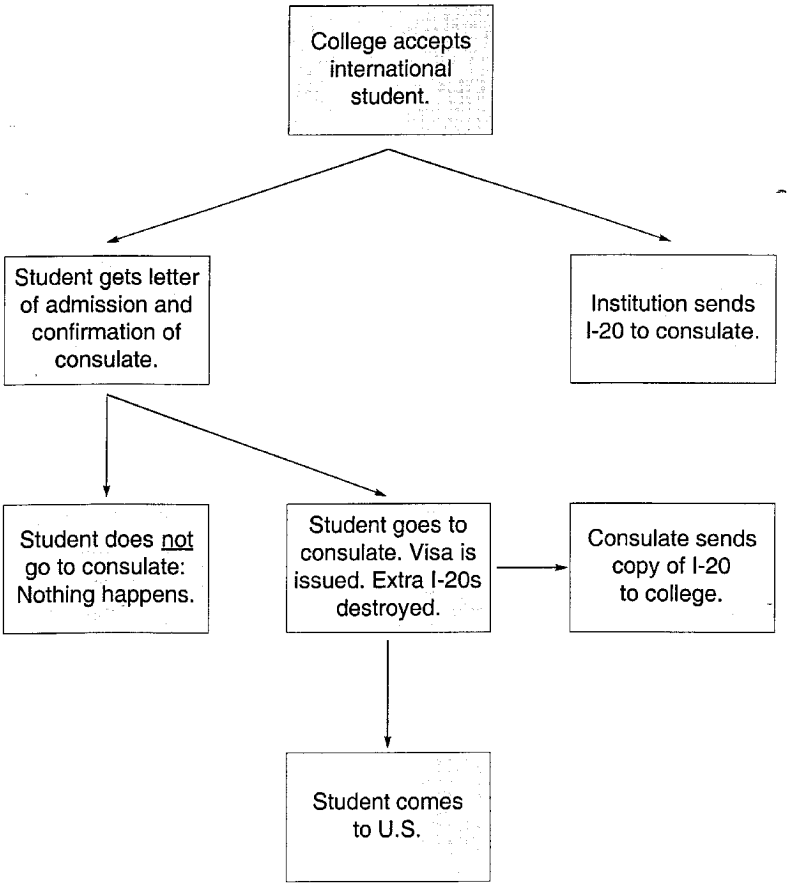
Delay the issuance of an I–20 form until after a prospective student from watch list countries has formally accepted admission.

Mandate a 30-day delay on issuance of all student visas for individuals from countries on watch list.

Testimony of Dr. David Ward
President, American Council on Education
Before the Senate Committee on the Judiciary
Subcommittee on Technology, Terrorism and Government Information
October 12, 2001

APPENDIX 2

Proposal to eliminate issuance of I-20s to students



Chairman FEINSTEIN. Thanks very much, Mr. Ward.

Mr. Tony Doonan is Vice President and Director, if I understand it, of the Automated Fingerprint Identification System at NEC Technologies. This is headquartered in Gold River, California, so welcome, sir. He is accompanied by Greg Spadorcio, who is Director of the Automated Fingerprint Identification System's Division.

NEC Technologies, AFIS Division, is one of the industry leaders in biometric technologies, having developed some of the first automated methods of identifying people by their fingerprint and palm print characteristics. They will testify about their work with law enforcement agencies and the FBI, and various technologies available to help verify identity.

Senator Kyl, you should know that when I was Mayor of San Francisco, NEC did a large system for us, and did it very well. They sent people over at that time, I think, from Japan to work with the city and put this system in. It was really, I think, a wonderful example of how the private sector can interface with the public sector and really provide a level of expertise that is not easily available to public sector people.

Mr. Doonan, welcome.

STATEMENT OF TONY DOONAN, VICE PRESIDENT, AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS; ACCOMPANIED BY GREG SPADORCIO, DIRECTOR, BUSINESS SOLUTIONS, NEC TECHNOLOGIES, INC., GOLD RIVER, CALIFORNIA

Mr. DOONAN. Madam Chairwoman, members, thank you very much for this opportunity. You actually stole my thunder there. I was going to comment that in 1983 I was associated with that project in San Francisco when, under your leadership, the San Francisco Police Department automated their fingerprint process. I at the time was with the California Department of Justice and worked closely with the police department in planning and implementing that system.

Chairman FEINSTEIN. We did this by bid, as I recall, and by far it really was the best, most comprehensive bid. I just want to say how important the software was to really get it developed in the right way up front and spent the time to do it.

Mr. DOONAN. That system has been a model for law enforcement for nearly 20 years. It is currently part of an interstate network that actually was responsible for identifying Mr. Resendez, the railroad killer. A latent fingerprint at one of the crime scenes was identified in that network.

Much of the technology that is in San Francisco today is applicable to the problems that you are discussing. Mr. Spadorcio is going to overview some concepts that we have developed that we think would help focus on the terrorism problem and how technology can be brought to bear.

We are also reaching out to Oracle, because we use their products, and Larry Ellison to see how we might, in concert, be able to bring solutions forward or ideas forward that might be able to address these issues.

Finally, for me, we also would be very happy to bring an operational system to the Capitol to demonstrate the technology to members and staff at a point that it was convenient for you.

Chairman FEINSTEIN. That would be very useful. Thank you very much.

Mr. DOONAN. I will turn it over to Mr. Spadorcio.

Mr. SPADORCIO. Thank you. Madam Chairwoman and members, thank you very much for being here. My discussion today highlights two programs that would benefit significantly from the introduction of biometrics by providing an added level of security to the issuance of passports and visas. Also discussed is a border control system that would verify each person at a port of entry against a database of known or suspected terrorists, compiled from data from Federal agencies and potentially other governments.

If you would refer to the application process for biometrics-enabled passport and visa diagram that I believe was provided in your package, I will walk through that quickly.

Ultimately, the traditional paper-based document passports and visas will be replaced by more secure smart card technology which will contain personal information, passport and visa information, and the digital biometric data of the card-holder; however, since substantial dollars have already been invested in the current passport and visa infrastructure, a phased approach that leverages the public's initial investment but yet adds significant security improvement to the passport or visa by adding biometric authentication.

Applicants for passports and visas will be required to capture a biometric sample in the form of a fingerprint that ultimately would be linked to the passport and visa records system. The passport collection centers—for example, the U.S. post office and the U.S. consulate office for visas—would process and transmit the fingerprint data electronically to a management database. The process would require all visa applicants to make their application in person, which is currently not a requirement of the visa process, so that their biometric sample could be collected.

The passport and visa management database of fingerprints would be used to compare against existing fingerprints of known or suspected terrorists prior to issuing or renewing a passport or visa. If a match against the database of known or suspected terrorists were not found, then the applicant could be granted a passport of visa consistent with current guidelines. If a match were found, the proper authorities would be notified for enforcement action.

The biometric information would ultimately be stored in a passport and visa management database so that it could be used for authentication and be accessed at any port of entry, consulate office, or other location that requires authentication of identity for passports or visas.

For approximately 30 countries that currently participate in the visa waiver pilot program, a fast-track immigration process could be enabled at ports of entry to allow holders of machine-readable passports who have pre-registered the biometric sample to pass through the immigration process rapidly. This approach would allow INS to focus their time and resources on those individuals that have not been pre-qualified and that may require additional time.

Chairman FEINSTEIN. Sir, I am going to interrupt you. You heard the Commissioner say that there is a law requiring that every plane be dealt with in 45 minutes.

Mr. SPADORCIO. Yes.

Chairman FEINSTEIN. If you had the biometric data in the passport of the system with respect to visa waivers, how much time would it take for that to register for each person coming off a plane.

Mr. SPADORCIO. And passing through some type of a checkpoint?

Chairman FEINSTEIN. Yes.

Mr. SPADORCIO. Literally seconds.

Chairman FEINSTEIN. Seconds?

Mr. SPADORCIO. Yes. At that point, it is really comparing the data in the passport versus the sample that was presented by the person. So it is making a one-to-one comparison of that person's identity at that moment, so it would be very rapid response.

Chairman FEINSTEIN. Thank you.

Mr. SPADORCIO. By utilizing the existing passport and visa, its information and infrastructure, the authentication system could be implemented quickly. In addition, smart card technology could be issued to augment the existing passport and eventually even replace the paper-based system without having to rebuild the entire authentication system.

There is also another diagram that is in your package. It is the port of entry diagram, and I will describe that quickly.

With the high volume of people crossing the U.S. border annually, providing for a secure border is paramount to our national security. However, immigration officials are often faced with dealing with competing demands: process the flow of people fast with minimal interference, but also with accuracy and diligence to ensure that no one is admitted that should not be admitted. While this is a heavy burden to carry, it has never been so important and vital to our country as today.

One way to ensure that the port of entry is secure from individuals that should not be admitted is through the use of a biometrics-enabled port of entry system. For passports or visas that are biometrically-enabled, the passport or visa would be scanned through a machine reader, as is currently done, and the passport- of visa-holder would then be requested to scan their finger and a query would be made to the passport and visa management database to verify that the person presenting the passport is the same person that was originally registered.

If a match were confirmed, the individual would be allowed to proceed through the port of entry. If a match could not be confirmed, then further investigation of the passport credentials would need to be conducted by enforcement personnel.

The passport and visa management database would be linked to an entry and exit system that would record all visa applicants' entry into the U.S. border, and would also be used to confirm their exit from the U.S. border. This system could either augment or replace the current I–94 form, which oftentimes is inconsistently collected by airlines and other transportation carriers, which results in erroneous visa exit data and makes the enforcement process almost impossible. A Web-based interface with a fingerprint scanner would be located at colleges and universities and other schools, and would require confirmation of students with visas' actual enrollment and participation in those programs.

For non-biometrics-enabled passports, visas and visa waiver program countries such as Canada, the goal would be to utilize a database of known or suspected terrorists and match it against people entering the U.S. at a port of entry. This system would be required for all entry into the U.S., unless the individual is already utilizing a biometrics-enabled passport, visa or smart card.

At the port of entry location, a person would be required to scan their finger to capture a fingerprint image that ultimately would be compared to the database. The port of entry system would be

designed to provide responses within a short time period after receiving the scanned fingerprint. For capturing fingerprints from cars, trucks or other transportation means, portable wireless scanners would be employed that could capture from one to multiple images for processing.

If a match were not found for a person's fingerprint at the port of entry system, they would be allowed to proceed through Customs as currently structured. If a match were found, enforcement agents would be notified for proper action.

In conclusion, while biometrics alone do not solve all the problems or issues associated with permanent or temporary immigration, it does add a significant level of trust to those documents that we rely on for entry to the United States. It also provides a means to ensure that a known or suspected terrorist would not be admitted into the United States. This alone is a worthy goal.

Thank you very much, and I would be glad to answer questions that you may have later.

[The prepared statement of Messrs. Doonan and Spadorcio follows:]

STATEMENT OF TONY DOONAN, VICE PRESIDENT, AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS; ACCOMPANIED BY GREG SPADORCIO, DIRECTOR, BUSINESS SOLUTIONS, NEC TECHNOLOGIES, INC., GOLD RIVER, CALIFORNIA

INTRODUCTION

With the growth of the global economy, the demand placed on the United States borders and its systems for managing permanent and temporary immigration is unprecedented. The Immigration and Naturalization Services (INS) conducted over 500 million inspections last year at nearly 300 land, air, and sea ports of entry. In approximately the same time period, the U.S. Department of State issued about 7 million U.S. Passports, over 6 million nonimmigrant visas, and close to 500,000 immigrant visas. It is clear that with these demands placed on the Nations borders, a more robust, secure and consistent form of border access is required.

Most countries, including the United States use traditional paper-based documents for passports and visas. Because of the passport and visas functionality and purpose, it is an important and trusted identification document that nations around the globe rely on. However, inherent to the design of the paper-based document system, it can easily be forged using advanced computer imaging and printing technologies. Ultimately, the confirmation of a person's identity in many situations relies on the information presented at the time of border crossing and the professional opinion of the border agent. A requirement of any secure border system is the ability to replicate the security screening process at every port-of-entry in a systematic and consistent manner, and since it ultimately will rely on human intervention, provide the appropriate technology to support the agent's efforts in trusting the document provided. Not surprisingly, national governments across the globe continue to search for a more secure method of providing passports and visa to avoid the security threats of a breached border.

This paper highlights two programs that would benefit significantly from the introduction of biometrics by providing an added level of security to the issuance of passports and visas, as well as provide the added benefit of an entry-exit tracking system for visa holders. The system would interface with the existing passport and visa process and thereby take advantage of the existing infrastructure. Also discussed is a border control system that would verify each person at a port-of-entry against a database of known our suspected terrorist or criminals that would be compiled of data from CIA, INS, FBI, DOD, Interpol and other cooperating agencies as specified.

BIOMETRICS ENABLED PASSPORTS

Ultimately, the traditional paper-based document passports and visas will be replaced by smart card technology which will contain personal information, passport and visa information, and the digital biometric data of the card holder. However, since substantial dollars have already been invested in the current passport infra-

structure, a phased approach that leverages the initial investment, but adds significant security improvement to the passport system by reducing the ability to tamper with the passport authentication process is described below:

1. When issuing or renewing a passport, an applicant would follow the established requirements for providing documentation, the appropriate identity information, passport photograph, and descriptive information. The applicant would also be required to capture a biometric sample in the form of a fingerprint that would be linked to the passport transaction number and ultimately become part of the passport authentication system linked to their passport.
2. The passport collection centers (Post Office, etc.) would process and transmit the biometric sample electronically to a main processing database where it would be compared against existing fingerprints of known or suspected terrorists or criminals prior to issuing or renewing the passport. If a match were not found, then the applicant would be granted a new passport or renewal. If a match were found, the proper authorities would be notified for enforcement action. It is estimated that the database would contain less than 500,000 fingerprints of known or suspected terrorists or criminals and be compiled from data from CIA, INS, FBI, DOD, Interpol, and other cooperating agencies.
3. The biometric information would ultimately be stored in a central database (or distributed database depending on design requirements, i.e. identical databases can be stored in additional locations to speed the system's response) for passport authentication and would be accessed at any port-of-entry, consulate office, or other location that requires authentication of an individual's passport.
4. To utilize the biometric capability, once a passport was scanned through a machine-reader, the passport holder would be requested to scan their finger and a query would be made on the central server database to verify that the person presenting the passport is the same person registered to that passport. If a match were confirmed, the individual would be allowed to proceed through the port-of-entry. If a match could not be confirmed, then further investigation of the passport credentials would need to be conducted.

By utilizing the existing passport, its information, and the passport infrastructure, the passport authentication system could easily be implemented today with little disruption and retooling of the existing infrastructure. In addition, smart card technology could be issued to augment the existing passport and eventually even replace the paper-based system without having to rebuild the entire authentication system. Both a smart card approach and the current passport systems could be implemented in parallel until the smart card infrastructure was fully developed.

An additional benefit of this system is that any country that has passports that utilize the machine-readable passport number, could participate in the authentication system. For the approximately 30 countries that currently participate in the Visa Waiver Pilot Program, a "fast-track" immigration process could be enabled at ports-of-entry to allow holders of machine-readable passports who have pre-registered their biometric sample with INS to pass through the immigration process rapidly. Essentially, their passport credentials will be authenticated by their fingerprint, which has already been "pre-qualified" by INS. This approach would allow INS to focus their time and resources on those individuals that have not been "pre-qualified", and that may require additional time to properly verify their credentials.

Part of the pre-qualification phase would be to match their fingerprint sample to the database of know or suspected terrorists or criminals. If there is not a match, then their biometric account would be enabled and they would have the privilege of using a fast track system with their biometrics. Each time a new fingerprint of known or suspected terrorists or criminals is added to the matching database, that specific fingerprint would be searched against the database of pre-approved passport and visa holders to ensure that there is not a match against the pre-approved database. If a match is found, that biometric account could be disabled and the appropriate enforcement personnel would be notified. Additional information could also be collected for statistical purposes.

Biometrics Enabled Port-of-Entry System

With the volume of people crossing the U.S. border annually, providing for a secure border is paramount to our national security. However, immigration officials are often faced with dealing with competing demands; process the flow of people fast, with minimal interference, but also with accuracy and diligence to ensure that no one is admitted that should not be admitted. While this is a heavy burden to

carry, it has never been so important and vital to our country as it is today. INS and other federal agencies have deployed several initiatives to help control and process the influx of people entering the U.S., in many cases without the benefit of coordination. One way to ensure that the port-of-entry is secure from individuals that should not be admitted is through the use of biometrics.

Currently, several databases of fingerprint data exist in different systems that do not necessarily coordinate or share important information that could help secure our borders. The goal of the biometrics enabled port-of-entry system would be to create a database of known or suspected terrorists or criminals from fingerprint information contained in INS, FBI, DOD, CIA, Interpol and potentially other agencies systems, that could be used to match against people at the port-of entry. The systems would require that an individual capture their finger on a scanning device as they pass through the port-of-entry for land, sea, and air locations. This system would be required for all entry into the U.S., unless the individual is already utilizing a biometrics enabled passport or visa.

At the port-of-entry location, a person would be required to scan their finger to capture a fingerprint image that ultimately would be compared to the database of known or suspected terrorist or criminals. The port-of-entry system would be designed to provide responses within second of receiving the scanned fingerprint. The output result from the matching process could be configured in several ways depending on the intended use. For walk-up situations, the system could be designed to activate turnstiles, gates, green or red lights, display based information, printed -material, or voice-activated commands. For capturing fingerprints from cars, trucks, or other transportation means, portable wireless scanners would be employed that could capture from one to multiple images for processing. The output result from the scanning device could include green or red lights, displayed information, or printed material.

If a match were not found for a persons fingerprint in the port-of-entry systems, then they would be allowed to proceed through customs as currently structured. If a match were found, the border agent would be notified for proper actions. The port-of-entry system would be very beneficial on the port-of-entry for countries that participate in the Visa Waiver Pilot Program. At a minimum, the system would be able to confirm that somebody in the database of known or suspected terrorist or criminals would not be able to make entry into the U.S., even if they provided fraudulent documents.

The system would be setup on a distributed basis to ensure redundancy capabilities and high speed processing. The central system would provide updates and housekeeping chores for each port-of-entry system to ensure accuracy and security.

BIOMETRICS ENABLED VISAS

The visa process would be very similar to the process described for passports. An applicant would be required to provide the appropriate information to the consulate office to process the visa as is currently required, however they will also be required to provide a biometric sample, such as a fingerprint at the time of their application. The fingerprint would be linked to the visa and passport record information. This process would require all visa applicants to make their application in person, which is currently not a requirement.

The consulate office would transmit the biometric sample electronically to a U.S. based main database where it could be compared against existing fingerprints of know or suspected terrorists or criminals prior to issuing or renewing the visa. If a match were not found, then the applicant would be granted a new visa or renewal. If a match were found, the proper authorities would be notified for enforcement action. It is estimated that the database would contain less than 500,000 fingerprints of known or suspected terrorists or criminals and be compiled from data from CIA, INS, FBI, DOD, Interpol, and other cooperating agencies, including local authorities.

The biometric information would ultimately be stored in a central database (or distributed database depending on design requirements) for passport authentication and would be accessed at any port-of-entry, consulate office, or other location that requires authentication of an individual's visa, including a web link for colleges, universities, and various schools to confirm visa participant's enrollment.

To utilize the biometric capability, once a visa was scanned through a machinereader, the passport holder would be requested to scan their finger and a query would be made on the central server database to verify that that the person presenting the passport is the same person registered to that visa. If a match were confirmed, the individual would be allowed to proceed through the port-of-entry. If a match could not be confirmed, then further investigation of the passport credentials would need to be conducted.

By utilizing the existing visa, its information, and the passport and visa infrastructure, the visa authentication system could easily be implemented today with little disruption and retooling of the existing infrastructure. In addition, smart card technology could be issued to augment the existing passport and visa and eventually even replace the paper-based system without having to rebuild the entire authentication system. Both a smart card approach and the current passport and visa systems could be implemented in parallel until the smart card infrastructure was fully developed.

Part of the pre-qualification phase would be to match the visa applicants fingerprint sample to the database of know or suspected terrorists or criminals. If there is not a match, then their biometric account would be enabled and they would have the privilege of using a fast track visa system with their biometrics. Each time a new fingerprint of a know or suspected terrorists or criminals is added to the matching database, that specific fingerprint would be searched against the database of preapproved passport and visa holders to ensure that there is not a match against the pre-approved database. If a match is found, that biometric account could be disabled and the appropriate enforcement personnel would be notified.

The fingerprint database would be linked to and entry and exit system that would record all visa applicant's entry into the U.S. border and would also be used to confirm their exit from the U.S. border. This system could either augment or replace the current I-94 form. One of the deficiencies of the I-94 form is that often times it is inconsistently collected by airlines and other transportation carriers. The biometrics enabled entry-exit system would be automatically updated with entry and exit information on a real time basis. The systems would be able to deactivate the biometric account for certain visa types once they have been scanned at the entry point, thus ensuring that the visa holder would not be able to reenter the U.S. border without obtain the proper visa or visa renewal. Enforcement personnel could easily receive reports on all expired visas with no exit data for their action. Additional information could also be collected for statistical purposes.

BIOMETRICS BACKGROUND

Since biometrics identifies people by unique human characteristics, such as a fingerprint, or facial recognition, it is considered highly reliable, accurate and secure. Most biometric technologies, like fingerprints, are beyond the "proof-of-concept" stage and are currently being implemented throughout the world to secure identity documents like passports, and national identification programs.

In recent years, the price of biometric technology and its infrastructure (processors, imaging electronics, and software) has dropped dramatically while the accuracy of biometrics technology has increased. Some biometrics technology, like have proven to be extremely reliable and accurate by law enforcement use for the last 30 years with largescale fingerprint applications. Many state and federal agencies are expanding the use of biometrics technology into applications aimed at entitlement fraud, driver licenses and state identification, and applicant processing.

ABOUT NEC TECHNOLOGIES' AFIS DIVISION

NEC Technologies' AFIS Division is recognized as an industry leader in biometrics technologies having developed some of the first and finest automated methods of identifying people by their fingerprint and palmprint characteristics. NEC Technologies AFIS Division provides identification solutions for law enforcement, government, and commercial applications requiring network security. Headquartered in Gold River, California, NEC Technologies, Inc., a wholly owned subsidiary of NEC Corporation is a leading manufacturer of computer peripherals and other technology products for the North American market.

ATTACHMENT 1

WHITE PAPER—THE BIOMETRIC SCENE

PREPARED BY: NEC TECHNOLOGIES

Automated Fingerprint Identification Systems (AFIS) Division

WHAT ARE BIOMETRICS

"A biometric is a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity"

Biometrics refers to the statistical analysis of biological characteristics. Biometric technologies are concerned with the physical parts of the human body or the per-

sonal traits of human beings. With today's technology, biometrics is used as an automated method whereby an individual's identity is confirmed by examining a unique physiological trait or behavioral characteristic, such as a fingerprint, or voice signature.

Physiological traits typically do not change; they are stable over time and somewhat unalterable and do not require frequent updates. A behavioral characteristic such as one's signature or voice is influenced by both controllable physical actions and less controllable psychological factors. Because behavioral characteristics can change over time, the biometric template must be updated each time it is used. Both techniques provide a significantly higher level of identification than traditional passwords.

Because biometric traits are unique to each individual, they can be used to prevent theft or fraud. Unlike a password, a biometric trait cannot be lost, stolen, or forgotten. Today's biometric identifiers include fingerprint, face recognition, facial thermo-gram, body odor, DNA, ear dynamics, keystroke patterns, palm print, retinal scan, iris patterns, signature, vein-scans, and voice patterns. Each of these biometric identifiers offers strengths and weaknesses for use in various situations.

In the security industry biometrics is regarded as providing the highest level of security. The methods for verifying an individual's identity are commonly broken down into the following three security levels:

Lowest level of security—something you have, such as a photo ID
Second level of security—something you know, such as a password or a personal identification number (PIN)
Highest level of security—something you do/ something you are, such as physiological and/or behavioral biometrics, including fingerprints, face recognition, signatures, etc.

HOW BIOMETRICS WORK

Most biometric systems operate in a similar fashion. The system captures a sample of the biometric characteristic for the purpose of enrolling the person in the system. During this enrollment phase some biometric systems may require a number of samples in order to build a profile of the biometric characteristic or to ensure that the system has captured the highest quality characteristic for later comparison purposes. Unique features are then extracted and converted by the system into a mathematical representation of the data. This mathematical representation of the data is then stored as the biometric template. The template may reside within the biometric system itself, in memory storage, such as a computer database, a smart card, or even barcode for later use.

When the user interacts with the biometric system to have their identity checked, the system will make a comparison of the stored template to the new offered biometric sample. If the template and the new sample match, the user is granted permission or access. Almost all biometric systems operate from this basic premise—a sample of the person's biometric data (finger-image) is captured and the biometric system decides if it matches with another confirmed sample of biometric data (fingerprint).

Because characteristics can change slightly over time, the biometric system must allow for some reasonable level of variation; typically a threshold is set that accounts for this variation. The comparison between the template and new sample must exceed the system's threshold before a match or confirmation is recorded. If not, the system will not record a confirmation or match and will not grant the user access or permission.

All biometric systems use the four-stage process of capture, extraction, comparison, and match (non-match). The core of the biometric system is the biometric engine, a proprietary process that extracts and processes the biometric data. This applies an algorithm to the extracted data. Essentially the system extracts the data, creates a template, and computes whether the data from the template and the new sample match.

The following process illustrates the way biometric systems typically operate:

Capture—a sample is captured by the system during enrollment
Extraction—data is extracted from the sample and a template is generated
Comparison—the template is then compared with a new sample
Match/Non-Match—the system determines if the features extracted from the new sample are a match or a non-match to the stored template

Within the biometrics industry, a distinction is made among the terms identification and verification. With identification, a sample is submitted to the biometric system during enrollment, this is stored as a template. Then during use, the system

receives a new biometric sample and then attempts to find out whom the sample belongs to, by comparing the sample against the entire database of templates in the hope of finding a match (this is known as a one-to-many or 1:n comparison).

Verification is a one-to-one (1:1) comparison in which the biometric system attempts to verify an individual's identity. In this example, a new biometric sample is captured and compared with the previously stored template. If the two samples match, the biometric system confirms that the applicant is who he/she claims to be. For a one-to-one comparison to work, the system must have access to some data that tells the system what record or template to compare against.

Identification—involves matching a sample against a database of many (Who is this?)

Verification—involves matching a sample against a database of one (Is this person who he/she claims to be?)

WHY BIOMETRICS

Government agencies, businesses, and individuals are recognizing the limitations of passwords and/or PIN numbers. As we see more examples of computer hacking, identity theft and other forms of fraudulent crimes, it is becoming more important to protect systems from unwanted intrusion. Biometric protected security offers a higher level of security because it verifies physiological or behavioral characteristics that are unique to each individual and are difficult to steal, alter, or otherwise forge. Biometrics systems, on average, can do a better job of protecting systems than other traditional forms of security.

A biometric record is a mathematical representation of an individual's unique characteristic (template), stored in electronic form. It cannot be used to reconstruct an image or to reveal a person's identity. When used for authentication, it serves as a comparison of the registered persons true form of identity—only one person can be registered with any unique biometric parameter. Compared to other methods of identity proof, biometrics is a tool that can actually enhance privacy and prevent abuse.

As more and more personal information is stored on computers, on network servers, within business systems, and healthcare facilities, it becomes increasingly important to ensure that only certain individuals have access to that information. Currently passwords are used almost exclusively for authentication on individual computers, networks, or across the Internet. While passwords are easy to develop and for the most part manage, they are far from being secure:

Passwords are easily forgotten

Passwords can be shared with others, allowing multiple individuals access to a secured environment

Multiple web accounts, email services, online stores, message boards, etc., require multiple password or worse, the same password for all environments

Typing passwords is inconvenient, bothersome, and often leads to poor password choice

Biometric authentication has the potential to solve many of these problems by eliminating passwords. By comparison, biometric characteristics (such as your fingerprint) offer enhanced convenience and security and are easy to use.

WHY FINGERPRINTS

Fingerprint technology has been utilized for decades to provide identification and verification of an individual. Today, the largest application of fingerprint technology is in Automated Fingerprint Identification Systems (AFIS) used by law enforcement agencies throughout the world. These are some of the largest and most complex fingerprint systems available, with hundreds of millions of fingerprint images in their systems. Most recently, finger-image technology has gained a significant following as the biometric technology most widely accepted and used for access control and enhanced security. Finger-image technology is currently in use for many applications, including military facilities, the Pentagon, financial institutions, large corporate networks, government and commercial laboratories, and almost anywhere that requires enhanced security.

The finger-image's strength is its user acceptance, convenience and reliability. It takes very little time (approximately the same time it takes to type-in a password) and effort for somebody to have their finger-image scanned and compared. Fingerimage identification is the least intrusive of all biometric techniques and one of the easiest to use. Users experience fewer errors when they use their finger-image versus many other biometric methods. In addition, a finger-image scanner requires

very little space on a desktop or in a machine. Several companies today have produced capture units small enough to fit on keyboards, embedded in a mouse device or laptop computer.

Finger-image technology also provides one of the lowest false acceptance ratios (FAR) (The probability that the system will incorrectly identify an individual or will fail to reject an individual when it should have) of all the biometric technologies, with less than one in a million. One of the biggest fears of fingerprint technology is the theft of someone's fingerprints. Concerns are that latent or residual prints left on the fingerprint scanner may be copied and used to gain access. However, good fingerprint identification devices will only detect live fingers and will not acknowledge fingerprint copies or other forgeries.

The practical applications of finger-image or other biometric technologies are diverse and ever expanding, however most non-law enforcement uses are for some type of access control. This will either involve the physical access of people to secure areas, or securing the access of privileged data or resources on servers. Whether securing government social benefit programs from fraud, preventing illegal immigrants from entering a country, or securing corporate networks from non-users, controlling access is the underlying strength of most biometrics, including finger-imaging.

BIOMETRICS APPLICATION EXAMPLES

AIR TRAVEL SECURITY

Biometric technology can be used to authenticate passengers and airline representatives for commercial air travel. The use of biometrics can ultimately be utilized for all aspects of travel from the initial reservation through baggage pick-up. The benefit to air travel is that once a person's identity has been verified at the initial check-in process and a biometric sample was captured, the biometric sample can be used to authenticate a person identity throughout the travel process. The cost to implement an air travel program would be negligible in comparison to the overall cost of travel.

DRIVER LICENSES AND STATE IDENTIFICATION

A driver license and identification card (ID cards) provides residents identification documents for host of uses where a person's identity needs to be confirmed. Driver licenses and ID cards are invaluable in our day-to-day life for providing identification to somebody who is usually unfamiliar to us or needs to verify that we are who we say we are. As such, the level of trust given to the driver license and ID card is enormous, and our reliance on these trusted documents must be ensured through a rigorous issuing process and the introduction of biometrics. A Department of Motor Vehicles (DMV) can easily introduce the use of biometrics to secure documents so that an individual cannot have a duplicate identity with state issued documents such as driver licenses and ID cards.

SOCIAL BENEFIT PROGRAMS

Social benefit programs are very vulnerable to fraud and misuse. Many social welfare departments throughout the world are utilizing biometrics to control access to the systems and reduce the fraud potential of these systems. A variety of technologies are deployed, however finger-image technology is most widely accepted. Many of these systems require large-scale AFIS type systems to manage the information and workflow requirements of these government organizations.

Another related area is the payment of benefits through the use of Electronic Benefits Transfer (EBT), which involves the use of a credit card type device that is secured with biometrics (finger-image template). The card can then be used to purchase items in retail stores tied to special point-of-sale smart card readers. Through the use of biometrics, the smart card devices can be secured from unauthorized users and for only allowed transactions. Biometrics is well placed to serve this market opportunity.

IMMIGRATION SYSTEMS

Illegal immigration and an increase in travelers throughout the world are requiring that immigration officials look for ways to control and manage the ever increasing volume of people. Biometrics is being employed in a number of diverse applications throughout the world to enable safe and easy travel. The U.S. Immigration and Naturalization Service (INS) are a major user and evaluator of biometric tech-

nologies for immigration control. Many governments are issuing immigration and work permits through the use of biometrics (mostly finger-image).

NATIONAL IDENTITY PROGRAMS

Governments are utilizing biometrics to identify citizens for national ID programs; these systems also lend themselves to voter registration systems to help prevent fraud during local and national elections. Often these systems involve storing a biometric template on a smart card or 2D card, which ultimately becomes a national identity document. Finger-image scanning is particularly strong in this area and programs are already underway in many countries.

FINANCIAL INSTITUTIONS

Financial institutions have been evaluating a range of biometric technologies for many years to control fraud and for general security issues. Automated teller machines (ATMs) and transactions at the point of sale are particularly vulnerable to fraud and are excellent candidates to be secured by biometrics. Related markets include remote access banking (Internet banking), remote access financial trading, financial document management, and other services that require a high level of security for both the institutions and consumers.

COMPUTER/NETWORK ACCESS

The single most active area for biometrics (finger-image) is to control the access to computer systems and network resources. This market area has enormous potential for enterprise wide applications. Also, as the biometrics industry migrates their technology to large-scale Internet applications to support, the use of biometric control will grow rapidly. The faster the user community accepts internet related transactions, the greater the need will become to secure this information from unauthorized uses. Biometrics will be a major source of security for these areas.

BUILDING PHYSICAL ACCESS CONTROL

The potential applications for access control are almost endless, from home use to nuclear power plants. Many organizations today are using biometrics to secure the physical movement of people throughout facilities or secure areas. Military facilities, theme parks, hospitals, offices, schools, government buildings, and other areas are employing biometrics to increase security. As security becomes more important for organizations, employers, governments and other groups, biometrics will be seen as a more acceptable and reliable tool.

INMATE MANAGEMENT SYSTEMS

Prisons are utilizing biometrics to ensure that prisoners are managed with secure identities. Prisoners' finger-images are enrolled during their registration into a prison system and are used throughout the system to manage access, court management, transportation, commissary privileges and even pharmacy programs. Perhaps the most beneficial to society is that an inmate's finger-image can be scanned and verified prior to release. A wide range of biometrics is now being deployed worldwide to secure prison access, home confinement, and regulate the movement of probationers and parolees, and manage court appearances. Many of the prison management systems can be tied to the large-scale AFIS systems that are employed by the law enforcement community for even greater accuracy and control.

TIME & ATTENDANCE SYSTEMS

Employers are always looking for ways to improve the recording and monitoring of employees time as they arrive at work, take breaks, and leave for the day. Someone "punching in or out" for someone other then themselves can deceive traditional "time clocks". The theft of "time" costs companies millions of dollars annually. Replacing the traditional "time clock" with biometrics helps to prevent abuses of a companies time management system. Once an organization develops a biometric time and attendance system, there are many opportunities open to them for reporting, employee monitoring, or other management systems.

BIOMETRIC MARKET POTENTIAL

Various organizations have devoted their resources to analyze the approximate size and velocity of the security market, including biometrics. The data varies, but the trend is consistent between all the studies—the biometric market is on a steep upward trend. Frost & Sullivan believes that the "U.S. User Authentication Device

Markets" generated revenues of over $200 million in 1999 and predicts that the figure will reach $2.6 billion by 2006.

The biometrics segment of the market is the most interesting and relatively new part of the security market. Up until the mid 1990's, the biometric market was almost non-existent commercially. Biometrics have become mainstream and more acceptable for a variety of government and commercial uses. Industry-wide standards are currently being developed, with participation from Microsoft, the International Biometric Industry Association (IBIA), BioAPI consortium, Intel and a host of other major players. Ultimately we will see the integration of biometric authentication technology into the next version of Windows, laptop computers, handheld computer devices, cell phones, and a host of other products thereby validating the technology and it application as a security tool.

ATTACHMENT 2

SUMMARY

As the demand for higher security for both passenger and air travel support personnel increase, the need for an accurate, reliable, and secure method of authenticating people becomes core to the security process. Airlines are looking into various ways to ensure that they can still provide a high level of service to their customers, while providing secure passage. Convenience and security can now go hand-in-hand by utilizing fingerprint technology to verify the identity of passengers and air travel personnel. Fingerprint technology can be used to authenticate passengers and airline representatives for commercial air travel. The use of fingerprint technology can ultimately be utilized for all aspects of travel from the initial reservation through baggage pick-up. A typical passenger authentication system can be easily deployed with proven biometric technology and available hardware and software systems. Figure 1 describes an overview of an airport authentication system.

AIRPORT AUTHENTICATION

The goal of this program is to ensure that the passenger's identity is confirmed throughout the airport experience. Even the Security Checkpoint can provide another level of authentication at which point additional security measures can be accomplished with cooperation of state and federal agencies. Airport security checkpoints can be implemented with the use of smart travel cards, proximity cards, key cards, bar codes, or other products that support fingerprint data. The fingerprint template that was created at the airline ticket counter can be sent via the network to match against a database of known or suspected terrorists or criminals. The database of known or suspected terrorists or criminals would need to be maintained in cooperation with Federal and State agencies. Any positive match in this scenario would alert authorities of a potential security issue and the passenger would not be allowed to pass through the security checkpoint. With the rapid acceptance of smart card technology around the globe, airline travel security and convenience can be enhanced with the issuance of smart travel cards for frequent travelers. Smart card technology can also be implemented and would allow enhanced security for use in a variety of ways for travel, including obtaining boarding passes, checking baggage, picking up baggage, updating and providing frequent flyer information, providing credit card information and verification of identity to obtain boarding passes, board aircraft and at security checkpoints.

The finger-image's strength is its user acceptance, convenience and reliability. It takes very little time and effort for somebody to have their finger-image scanned and compared. Finger-image identification is the least intrusive of all biometric techniques and one of the easiest to use. Whether protecting airline travel, social benefit programs from fraud, or preventing illegal immigrants from entering the country, the underlying strength of NEC's finger-imaging technology is its core algorithms and its ability to verify authorized access controls.

AIRPORT SECURITY APPLICATIONS

PASSENGER AUTHENTICATION

The use of fingerprint technology can ultimately be utilized for all aspects of travel from the initial reservation through baggage pick-up. A typical passenger authentication deployment is described in Figure 1 and listed below:

1. The passenger enters the airport and proceeds to the ticket counter. The ticket agent will access the airline passenger reservation record and confirm the boarding details such as flight, gate and seat assignment. The ticket agent will also process

checked luggage and other necessary preflight details. At this point the system prints a boarding card and any baggage receipts.

2. The passenger will be asked to provide appropriate identification (state or other government issued photo identification, passport, etc.) and will be asked to place their finger on the fingerprint scanner. An image will be captured and processed into a fingerprint template. The ticket agent will then enter the flight number and gate code into the fingerprint scanner workstation. The fingerprint template that was just created will be sent via the network to the appropriate gate and stored in the cache of the fingerprint workstation at the gate. The use of this system should not impact the time it currently takes the airline ticket counter to process a passenger's ticket.

3. The passenger will then proceed to the security check where they will be asked to provide appropriate picture identification and their boarding pass. After the security check, the passenger will proceed to their departure gate.

4. At the departure gate and during the boarding process, passengers will hand their boarding pass to the ticket agent and then be asked to place their finger on the fingerprint scanner. The fingerprint workstation will capture a new finger-image and process it into a new fingerprint template and then conduct a search of the passenger database for a match on each passenger. If a match is found, the passenger will be allowed to board the plane. The finger image verifies the passenger's identity as the same person that received the boarding pass from the ticket agent. If a match is not found, then alternate identification methods will be deployed. This system will process the fingerprint data in seconds.

5. Airline representatives will assign flight representatives to individual flights through a developed user interface. The flight representatives would be required to scan their finger prior to boarding the aircraft to ensure that they are employees of the airlines and that they are actually scheduled for the assigned flight.

6. Passengers transferring from other flights will proceed to the appropriate departure gate where the process performed at the original ticket counter will be repeated for checking identification and capturing a fingerprint (Note: transferring passengers can be issued boarding passes with their fingerprint template stored on either a magnetic stripe, two dimensional barcode, or other supporting technology and not have to re-register at the gate prior to boarding). Each transfer would be handled as a separate event and require the passenger to show proper identification to the ticket agent and register their fingerprint prior to boarding. The fingerprint security system can be developed to automatically route the appropriate fingerprint templates to other airports and departure gates, as the infrastructure is developed to support this workflow.

117. Passengers that already have reservations and would prefer to proceed directly to the boarding area to obtain their boarding pass may do so as current security regulations permit. The passenger would follow the same check-in procedures outlined for the ticket counter at the departure gate.

8. Once the plane has arrived at its destination, the captured fingerprint templates that were used to verify the passenger's identity to board the aircraft would be purged from the respective airlines database.

SECURITY CHECKPOINT AUTHENTICATION

The Security Checkpoint can provide another level of authentication at which point additional security measures can be accomplished with cooperation of state and federal agencies.

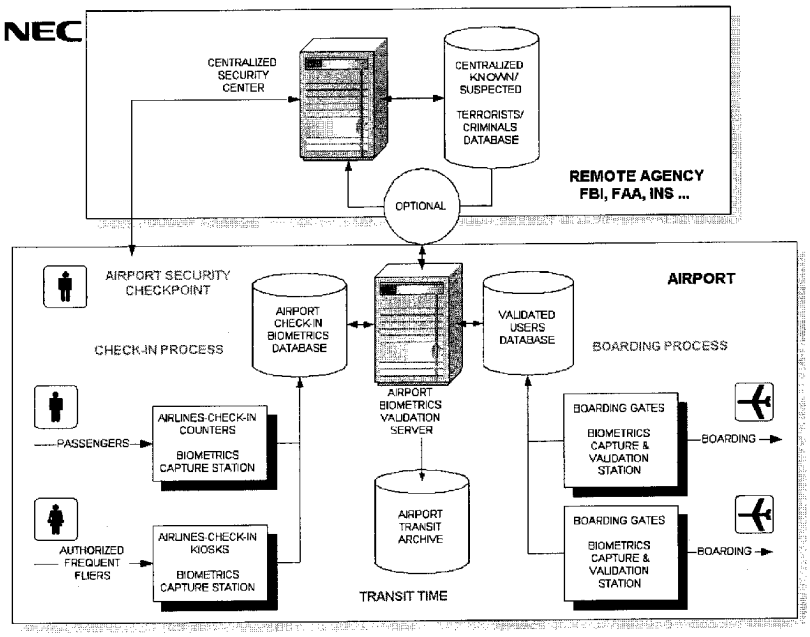
1. At the airline ticket counter, passengers will be asked to provide appropriate identification (state or other government issued photo identification, passport, etc.) and will be asked to place their finger on the fingerprint scanner. A finger-image will be captured and processed into a fingerprint template. The fingerprint template will be sent via the network to a matching server containing a database of known or suspected terrorists or criminals fingerprint templates and used to match against each passenger fingerprint template that was created during the ticketing process. The use of this system should not impact the time it currently takes the airline ticket counter to process a passenger's ticket. The database information will be passed to the security checkpoint system for authenticating passengers.

2. The ticket counter representative will then provide to the passenger a smart travel card, proximity card, key card, bar code, or other product that supports finger-image data for use at the security checkpoint. Passengers will proceed to a gated or turnstile security checkpoint where they will be prompted to provide their smart travel card, proximity card, key card, bar code, or other product that supports finger-image data to an electronic reader. The passenger will then place their finger on a scanner where a new fingerprint will be captured and compared to the finger-

print on the smart travel card, proximity card, key card, bar code, or other product that supports fingerimage data that was provided at the ticket counter. All approved passengers (no match found in the database) fingerprint templates will be sent to the appropriate gate fingerprint system for confirmation of passenger boarding. If during the matching process on the known or suspected terrorist or criminal database, a match is found of a ticketed passenger and a record in the database, the security checkpoint system will be alerted.

3. After the security checkpoint, the passenger will proceed to their departure gate. At the departure gate and during the boarding process, passengers will hand their boarding pass to the ticket agent and then be asked to place their finger on the fingerprint scanner. The fingerprint workstation will capture new finger-image and process it into a new fingerprint template and then conduct a search of the passenger database for that flight. If a match is found, the passenger will be allowed to board the plane. If a match is not found, then security will be deployed to resolve the issue. This process will take less time then it currently takes to confirm passenger's identity through traditional means.

Figure 1 - Airport Security Utilizing Fingerprints Workflow



TRAVEL SMART CARDS

Travel smart cards issued utilizing a unique numbering sequence similar to that adopted by Visa and MasterCard that identifies the individual's account and the issuing organization would provide added functionality over traditional frequent travel programs or conventional smart card programs. The unique numbering system would allow the travel smart cardholder to extend its use for authentication at any security checkpoint, ticket counter, kiosk, or departure gate. Frequent travel programs, affiliations and alliance members can use the same travel smart card instead of the traditional frequent travel program cards. This system also has the a potential for reduced costs through consolidated travel program management, program adoption, and increase the speed at which travelers could access services.

By applying a unique numbering system to travel smart cards, frequent traveler programs could be streamlined, consolidated, and ultimately managed and issued by a third party organization and utilized by all organizations with frequent travel programs. The unique number assigned to an individual account would ensure that the

associated fingerprint and account is registered only once in the record management system. This approach will allow for faster authentication for secure usage. The registration process would be a rigorous process to ensure the person's identity, credit card information, physical address, and biometrics (finger-image templates, and other) data are accurate and reliable. The travel smart card would become a trusted source of information when presented with a Personal Identification Numbers (PIN) and or biometrics (finger-image technology).

The benefits of utilizing travel smart cards is that frequent travelers preferences could be embedded in the travel smart card along with the individual's descriptive information, travel requirements, issuing organization information, travel program affiliations and alliance information, credit card, other relevant information, and biometric (finger-image template) data. The travel smart card can be used in a variety of ways for travel, including obtaining boarding passes, checking baggage, picking up baggage, updating and providing frequent flyer information, providing credit card information, and verification of identity to obtain boarding passes, board aircraft, and at security checkpoints. A travel smart card would help to speed-up the transaction time it takes to confirm somebody's identity and process their transaction.

1. A frequent traveler completes the registration process (paper-based, web based, kiosks at travel locations, etc.) that includes descriptive information, choice of primary frequent traveler programs, secondary frequent traveler programs, travel preferences, credit card information (optional), and other information as subscribed or required. To add the biometric feature to the travel smart card, a frequent traveler will be asked to place their finger on the fingerprint scanner. A finger-image will be captured and processed into a fingerprint template. The fingerprint template will be captured to the travel smart card and also sent to a matching server containing the main database of known or suspected terrorists or criminals fingerprint templates. A check of the database will be conducted on a one-to-many (1:N) basis to ensure that every travel smart card cardholder is not represented in the known or suspected terrorist or criminal database.

2. Since each travel smart cardholder has a unique number assigned to their account, any updates to the database of known or suspected terrorists or criminals fingerprints can easily be searched across the travel smart cardholders account. If a match is found, the appropriate authorities will be notified and the travel smart card would become invalid and placed on alert.

3. Frequent travelers entering the airport will proceed to a kiosk, ticket counter, or directly to the assigned gate. At the gated or turnstile security checkpoint the passenger will be prompted to provide their smart travel card to the electronic reader. The passenger will then place their finger on a scanner where a new fingerprint will be captured and compared to the fingerprint on the smart travel card. All approved passengers (no match found in the database) will proceed to their appropriate gate.

4. At the departure gate, the smart travel cardholder will obtain their boarding pass from the attendant by following the same check-in procedures outlined for the ticket counter. During the boarding process, passengers will hand their boarding pass to the ticket agent and then be asked to place their finger on the fingerprint scanner. The fingerprint workstation will capture a new fingerimage and process it into a new fingerprint template and then conduct a search of the passenger database for that flight. If a match is found, the passenger will be allowed to board the plane. If a match is not found, then security will be deployed to resolve the issue.

4. Once the plane has arrived at its destination, the captured fingerprint templates that were used to verify the passenger's identity to board the aircraft would be purged from the respective airlines database.

ADDITIONAL AIRPORT SECURITY OPTIONS

Physical Access Control Throughout Airport
Airlines Human Resource Systems
Time and Attendance Systems
Time and Attendance Systems integrated with Physical Access Controls

Chairman FEINSTEIN. Thank you very, very much. That was very helpful.

Our final witness is Paul Collier. He is the Executive Director of the Biometrics Foundation. He is a founding member of the International Biometrics Industry Association and served on its board of directors for two years. He is here to speak about some of the tech-

nologies available to identify and capture terrorists before they enter this country and disappear.

Please proceed, Mr. Collier.

STATEMENT OF M. PAUL COLLIER, EXECUTIVE DIRECTOR, BIOMETRICS FOUNDATION, GAITHERSBURG, MARYLAND

Mr. COLLIER. Thank you, Madam Chairwoman and members of the subcommittee, for inviting me to be a part of this distinguished panel today. My testimony will focus on how the Federal Government has used biometric technology in the past and how the technology available today can offer a significant advance in controlling access at our borders and serve as an effective tool in our mission to combat terrorism.

A biometric is a quantitative measurement of a unique human attribute or behavioral characteristic, such as fingerprints, face, voice, iris recognition, hand geometry, et cetera. Using fingerprints as an example, a finger is placed on a sensor and then scanned. The image of the fingerprint is then processed by a series of algorithms which convert it into a binary representation or template. This template is then compared to a reference template stored either on a computer or card-based storage data medium. Like most biometrics, you cannot reverse-engineer this binary representation to re-create the scanned image.

Further, biometric methodologies can be categorized as two types: contact and passive. A contact biometric is one that requires an individual to interact with or touch a sensor, such as fingerprint or a hand geometry scanner. A passive biometric is one that does not require any action on the part of the individual, such as facial recognition.

Biometrics have been used in many civil and government programs worldwide for over 10 years. They have been very effective in reducing fraud, eliminating multiple identities, and securing access to sensitive areas. These wide-scale deployments have served as a real-world proving ground for this technology and involve many millions of people. Knowledge gained from these programs and applied to improvements and cost reductions helped produced many of the commercial products available today.

Traditionally, the primary applications for biometrics in the Federal Government and military have been physical and logical access and fraud reduction programs. Though many successful pilots and proof of concept studies have been done, wide-scale deployment has been slow. A complete list of all the Federal Government and military applications would keep us here probably for several days, but I have highlighted a few examples.

The U.S. Department of Defense initiated a real-time automated identification system, known as RAPIDS, and the Defense Enrollment and Eligibility Reporting System, DEERS, as its positive identification system for the Department of Defense for all active and retired military personnel. At the same time, they implemented a program known as Operation Mongoose which was designed to combat military retirement fraud primarily overseas.

The Department of Defense also initiated a program known as the Biometric Identification System, or BIDS, which is actually an evacuation system that is deployed in South Korea that can be

used in the event of our need to evacuate U.S. personnel from that theater. The National Security Agency uses it for access control to sensitive areas and systems.

The Department of Energy has used biometrics for years to control access to nuclear plants. The Immigration and Naturalization Service's IDENT program which was discussed earlier, as well as their INSPAS program, is used to speed passengers through immigration screening.

The Federal Bureau of Investigation uses biometrics for access control at the Clarksburg, West Virginia, facility; the General Services Administration for logical access to computer networks. The State Department—we have discussed the border crossing card project. The Secret Service initiated the Treasury Recipient Integrity Program, or TRIP, as an anti-fraud mechanism for recipients of Federal entitlement monies.

In addition to projects such as these, both the Federal Government and military are in the process of evaluating and deploying commercial off-the-shelf biometrically-based log-on products to protect computers, networks and sensitive data.

It should be noted that the Federal Government, in partnership with industry, has made a significant contribution to the evolution of biometric technology. Biometrics would not have advanced to their present level without the help of the Department of Defense, the National Security Agency, the Departments of Justice, Energy, Treasury, and the National Institute for Standards and Technology.

Despite the fact that the United States has pioneered the development of many biometric technologies, we lag behind the rest of the world in their deployment. Many other countries use biometric authentication features in national identification cards, border-crossing documents, voter registration, drivers' licenses, et cetera.

Domestically, some efforts have been made to incorporate biometrics into government-issued identification cards, but they have fallen short of realizing the full potential of the technology which was pointed out earlier today.

An example: We have approximately 11 million drivers' licenses in the United States and 5 million border-crossing cards, almost, already issued which include biometric data. Currently, there are no systems in place to read the biometric data and authenticate the card-holders. The use of biometrics in the border entry application process would significantly—

Chairman FEINSTEIN. Excuse me. You are saying that there is this huge investment already in drivers' licenses and border-crossing cards that have the biometric data on the card, but there is no system to read that?

Mr. COLLIER. Correct. There are several companies that have produced products to do so, but the products have not been purchased and deployed by the government agencies, whether they be State or Federal.

The use of biometrics in the border entry application process would significantly augment security when compared to current lookout list systems. Databases such as fingerprints and photographs already exist worldwide. Encoding biometric data in passports, visas, identification cards and other travel documents can

provide positive identification of the bearer and speed the entry process, as was pointed out earlier.

At the same time, passive biometric technologies such as facial recognition can play a significant role as a surveillance tool at our airports, ports of entry, and virtually any potential high-threat-condition facility or event. This technology is easily integrated into many existing surveillance camera systems, and unlike individual profiling, biometric technology is neutral, as opposed to a subjective assessment that is prone to human error.

Biometrics alone are not a panacea, nor can any single biometric meet all application requirements. Successful applications require the selection of the proper technology that can be integrated into existing solutions. Biometrics offer great promise for a significant advancement in security, while protecting our privacy and maintaining a low impact on how we go about our daily activities, and play a significant role in our Nation's critical infrastructure, and have applications in virtually all aspects of our society.

As an emerging technology, significant advances have been made in establishing industry standards—

Chairman FEINSTEIN. Could you wrap it up, Mr. Collier, because we need to move on?

Mr. COLLIER. —and addressing issues of interoperability. The efforts of the Biometric Consortium, co-chaired by NSA and the National Institute of Standards and Technology, the International Biometric Industry Association, the Biometric Foundation and West Virginia University have all played an important role.

In closing, for biometric technologies to realize their full potential will require an accelerated pace in the work of these institutions. In light of the events of September 11, wide-scale deployment of biometric solutions becomes more critical and time is of the essence.

Thank you, Madam Chairman.

[The prepared statement of Mr. Collier follows:]

STATEMENT OF M. PAUL COLLIER, EXECUTIVE DIRECTOR, BIOMETRICS FOUNDATION, GAITHERSBURG, MARYLAND

Madame Chairman, members of the subcommittee, thank you for inviting me to be a part of this distinguished panel. My testimony will focus on how the federal government has used biometric technology and how technology available today can offer a significant advance in controlling access at our borders and serve as effective tool in our mission to combat terrorism.

A biometric is quantitative measurement of a unique human attribute or behavioral characteristic such as fingerprints, face, voice, iris, hand geometry, etc. Using fingerprints as an example; a finger is placed on a sensor and then scanned. The image of the fingerprint is then processed by a series of algorithms, which convert it into a binary representation, or template. This template is then compared to a reference template stored either on a computer or card based data storage medium. Like most biometrics, you cannot reverse engineer this binary representation and recreate the scanned image.

Biometric methodologies can be categorized as two types, contact and passive. A contact biometric is one that requires an individual to interact with or touch a sensor such as fingerprint or hand geometry. A passive biometric is one that does not require any action on the part of an individual such as facial recognition.

Biometrics have been used in many civil and government programs worldwide for over ten years. They have been very effective in reducing fraud, eliminating multiple identities and securing access to sensitive areas. These wide-scale deployments have served as real world proving grounds for this technology and involved many millions of people. Knowledge gained from these programs and applied to improvements and cost reductions helped produce many of the commercial products available today.

Traditionally, the primary applications for biometrics in the federal government and military have been physical and logical access control and fraud reduction programs. Though many successful pilots and proof of concept studies have been done, wide scale deployment has been slow.

A complete listing of all federal government and military applications would be quite extensive, but a few examples of successful deployments are:

US Department of Defense—Real-time Automated Identification System (RAPIDS) & Defense Enrollment and Eligibility Reporting System (DEERS) (positive identification)

US Department of Defense—Operation Mongoose (military retirement anti-fraud)

US Department of Defense—Biometric Identification System (BIDS) (evacuation system deployed in South Korea)

National Security Agency—access control to sensitive areas and systems

US Department of Energy—access control in nuclear plants

Immigration and Naturalization Service—IDENT System (illegal entry control on our southwest border)

Federal Bureau of Investigation—access control at Clarksburg, WV facility

General Services Administration—logical access to computer networks

US Department of State—Border Crossing Card Project

US Secret Service—Treasury Recipient Integrity Program (TRIP) (anti-fraud)

In addition to projects such as these both the federal government and military are in the process of evaluating and deploying commercial-off-the-shelf biometric logon products to protect computers, networks and sensitive data.

It should be noted that the federal government, in partnership with industry has made a significant contribution to the evolution of biometric technology. Biometrics would not have advanced to their present level without the help of the Department of Defense, National Security Agency, Department's of Justice, Energy, Treasury and the National Institute for Standards and Technology.

Despite the fact that the United States pioneered the development of many biometric technologies, we lag behind the rest of the world in their deployment. Many other countries use biometric authentication features in national identification cards, border crossing documents, voter registration, driver's licenses, etc. Domestically, some efforts have been made to incorporate biometrics into government issued identification cards but they have fallen short of realizing the full potential of the technology. In example; we have approximately 11 million driver's licenses and five million border crossing cards already issued which include biometric data. Currently, there are no systems in place to read the biometric data and authenticate the cardholders.

For instance, the use of biometrics in the border entry application process would significantly augment security when compared to current "look-out" list systems. Databases such as fingerprints and photographs exist worldwide. Encoding biometric data in passports, visas, identification cards and other travel documents can provide positive identification of the bearer and speed the entry process.

At the same time, passive biometric technology such as facial recognition can play a significant role as a surveillance tool at our airports, ports of entry and virtually any potential "high threat condition" facility or event. This technology is easily integrated into many existing surveillance camera systems. Unlike individual "profiling", biometric technology is neutral as opposed to a subjective assessment that is prone to human error.

Biometrics alone is not a panacea, nor can any single biometric technology meet all application requirements. Successful applications require selection of the proper technology that can be easily integrated into existing solutions. Biometrics offer great promise for a significant advancement in security while protecting our privacy and maintaining a low impact on how we go about our daily activities. Biometrics can play a significant role in the protection of our Nation's critical infrastructure and have applications in virtually all aspects of our society.

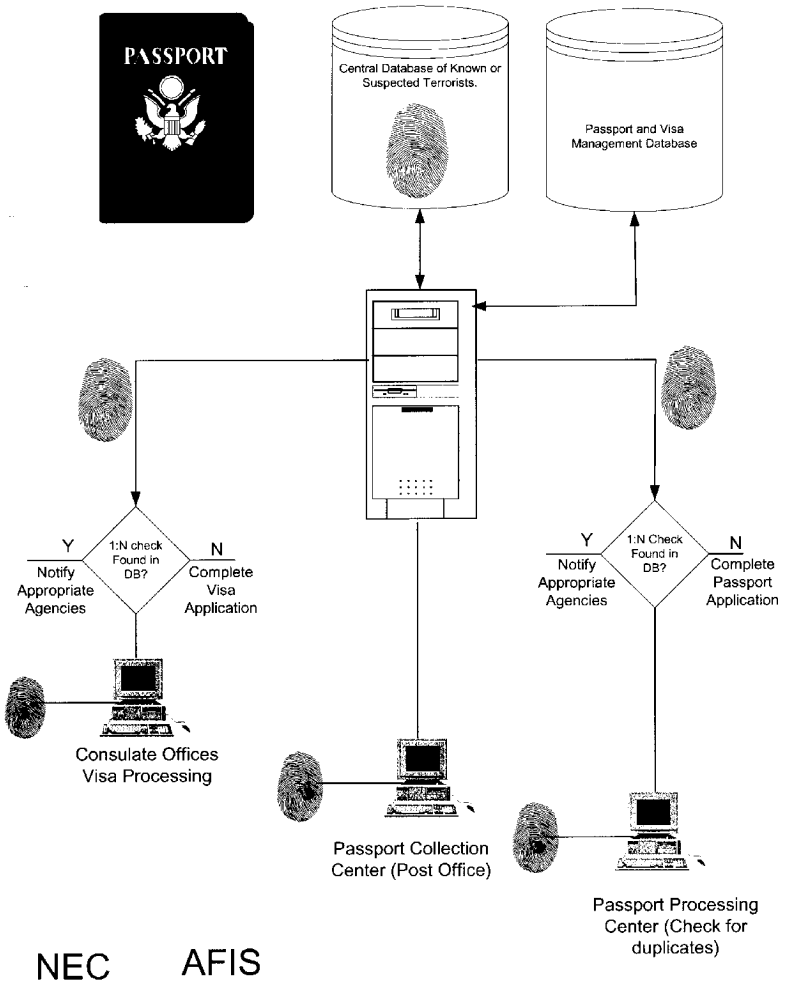
As an emerging technology, significant advances have been made in establishing industry standards and addressing issues of interoperability. The efforts of the government's Biometric Consortium, co-chaired by National Security Agency and the National Institute for Standards and Technology working with the General Services Administration, the International Biometric Industry Association, The Biometric Foundation, West Virginia University—Center for Identification Technology Research along with it's other academic partners and the member companies of the BioAPI Consortium have been instrumental bringing the industry to it's present level. To date, most of this work has been accomplished with little, or no funding from the government or outside institutions.

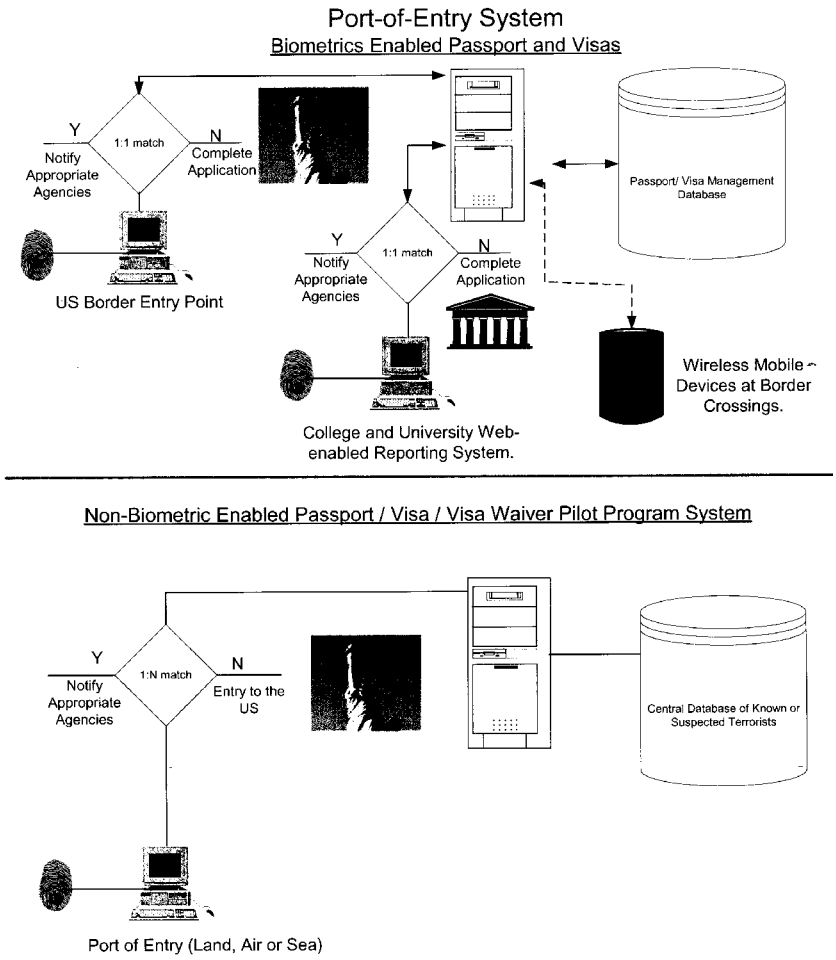
For biometric technologies to realize their full potential will require an accelerated pace in the work of these institutions. In light of the events of September 11th, wide

scale deployment of biometric solutions becomes more critical and time is of the essence.

Thank you Madame Chairman

Application process for Biometrics Enabled Passports and Visas





NEC AFIS

Chairman FEINSTEIN. Thank you very much. Let me thank everybody. I think the testimony was excellent.

Mr. Ward, let me particularly thank you and your organization for really being helpful in this. However, I don't want you to think, because I sent that letter, that I don't believe that there should be a fee system and that the fees should be collected by the schools and sent into the government, because I do believe that. I think that is extraordinarily important for everybody to understand.

I would like to go on to Mr. Doonan. I would like to ask a question and hopefully you will be able to give me some ball-park answer, and that is the cost of implementing the programs recommended in your written statement. You recommend the imple-

mentation of three new programs—a biometric-enabled U.S. passport, a biometric-enabled port of entry system, and a biometric-enabled visa system.

Do you have a ball-park estimate of the cost of implementing these systems, software and hardware?

Mr. DOONAN. It is really quite difficult. First of all, we would have to define how large is the database of suspected or known terrorists because you have to put their fingerprint records in it, and the size of the database, as you know from your experience in San Francisco, relates largely to the cost.

Next, we would have to determine how quickly we could establish the biometrically-enabled documents because once you have that, the process of entering and leaving the country is really a one-to-one verification of the fingerprint and does not require much technical horsepower, if you will.

The real problem comes from the visa waiver program, where you have large numbers of people that are crossing the border and you have to search every one of them against that known or suspected terrorist database. So until we were able to sit down with appropriate Government representatives and try to define the scope of this thing and have some implementation plan, it is very difficult to say.

Now, I believe that Senator Bond had referenced recently $500 million. I would not quarrel with that number at all.

Chairman FEINSTEIN. What is the best biometric data to use? Our purpose here is not to present a problem for the legitimate citizen, but our problem is to get at the person that may, by virtue of his associations, his or her background, criminal record, cause harm to the United States. Is a fingerprint or is a facial I.D. the best biometric information for that purpose?

Mr. DOONAN. We are in the process of developing facial recognition technology. As Mr. Collier said, that is typically a passive biometric. The real issue is, on a one-to-one verification basis, that technology may be very reliable, but if you are searching a large database, I don't know that anybody has accurate statistics about how accurate it would be.

The fingerprints have been historically the most acceptable biometric in terms of accuracy and availability. Also, on facial recognition, I guess I would be concerned if 19 people were willing to kill themselves to do what they did on September 11, they might be able to significantly change their facial profile and actually defeat the system.

Chairman FEINSTEIN. I remember conversations that I had with NEC about fingerprints and improving fingerprint technology. Has the state of the art advanced to the extent that a single print is now adequate?

Mr. DOONAN. We would probably recommend the storing of two fingerprints in the database, one because it gives you a backup in case the other one is damaged.

Chairman FEINSTEIN. It gives you what?

Mr. DOONAN. A backup in case one of them is damaged. Also, in terms of designing a system, if you have two fingers, it is less expensive to search the entire database than if you have one. So there are considerations, but in terms of accuracy on a one-to-one

basis, you can be virtually given hundred-percent accuracy. When you are searching the database, it is in the very, very high 90-percent range.

Chairman FEINSTEIN. I would like to ask Mr. Collier this question: How would you compare the biometric systems used on the United States side of the border with that being used on the Canadian side?

Mr. COLLIER. The Canadians have not deployed a full biometric system for controlling the border. They have a few systems designed for province-level identification cards, as well as, again, entitlement programs.

Chairman FEINSTEIN. Let me just stop you. It is my understanding Canada passed an anti-terrorism package of $91 million that includes $8 million for some 65 fingerprint scanners to be set up at high-risk border crossings. That is essentially what I am talking about.

Mr. COLLIER. I don't believe they have deployed yet. I was in a conversation actually with someone last week and I understand that they were looking to the United States to see what we were going to do first.

Chairman FEINSTEIN. I see.

Senator Kyl has to leave, so I would like to defer to him.

Senator KYL. Thank you very much, and I will just tell you I have to leave here in about 6 or 7 minutes.

First of all, thank you. Mr. Camarota, you had some very good suggestions. David Ward, let me ask you just a couple of questions and then I have a general question regarding the same subject we were just discussing, the digital facial versus fingerprint.

Just to give us a point of reference, at the University of Wisconsin what is the out-of-state tuition that a foreign student would pay?

Mr. WARD. Well, last year it would have been about $14,000 and this year it is going to be $18,000.

Senator KYL. When does the—

Mr. WARD. Senator, if I could interrupt, many of these students do get teaching assistants or scholarships that help.

Senator KYL. Sure, sure. I am just trying to get a rough idea.

When would they pay their tuition, or at least a part of it?

Mr. WARD. As they register.

Senator KYL. Okay. One of the concerns that you expressed about the INS approach to a fee—and I agree with Senator Feinstein that the student and the university have to bear part of the expense, just like American businesses do. For someone that they bring in to assist them, they pay a pretty healthy fee for that, and I don't think that is unreasonable to ask these students to do.

You have said the plan would seriously undermine the ability of most foreign students to enroll at American colleges, and I think that may be a little overstated. You say the plan would require students to pay using either the Internet, a credit card or American dollars, and many international students don't have access to credit cards, American dollars or the Internet.

Now, it seems to me that anybody that is going to be coming to the United States could easily get access to American dollars. I

mean, they are going to be in a country where you can exchange whatever they have for American dollars.

In any event, if that is too hard, there is nothing to prohibit the university from paying the fee and then collecting it from the student once they arrive. Of course, they are obviously going to be good credit risks or you wouldn't have them come.

So I think it would be helpful to us for you to work out a system that would be easiest for universities and other schools to implement, least cost, most efficient, and share that with us, because nobody wants to impose something that is not going to work. Come up with an idea that will work, with the assumption that there has to be some expense borne by the student and the institution.

Mr. WARD. Could I ask my colleague if he has any reaction? He is on the front line of—

Senator KYL. Sure, but may I do this? I apologize for this, but unfortunately I have a live radio interview I have to do and I have to leave here in just a minute, but we would appreciate anything in writing. Give us a call, stop by and visit, or just any ideas you have, because I am sure you can come up with something that we can make work. So thank you.

To any of the rest of you here, we have different needs. Both Senator Feinstein and I, and actually Senator Cantwell as well, want to make it very easy for people to get back and forth, because we are all from border States and for commerce and all the other reasons we are for that.

Secondly, we know that there are different needs here. We have photographs of a lot of terrorists, but we don't have fingerprints. So even though a fingerprint system may be best for most honest people and Americans and a lot of people coming in here from foreign countries, it may not work best for the one thing we are really focusing on here, and that is the terrorist.

So given that question and the fact that you have existing databases that are very large with certain kinds of systems, what would you recommend? Is it possible to make different kinds of systems work together, or does there have to be one integrated system? What would you recommend in that regard?

Mr. COLLIER. Senator Kyl, the good news is that the Biometric Consortium and the National Institute for Standards and Technology and their standards efforts have come up with a common biometric exchange file format. That would allow you to put either multiple or layered biometrics of many types on a single document or in a single database that would give you the groundwork for interoperability.

Additionally, most biometrics have small, reduced template sizes for one-to-one verification. That means it is not a real estate issue anymore with the amount of data storage you have got either on a card or in a database.

Senator KYL. And is that going to be readable? The problem we have understood here is that you can have the fraud-proof document, perhaps, but we don't have the readers.

Mr. COLLIER. Well, there are readers out there. Fingerprint readers have actually, I think come down inexpensively for smart card applications. Some of the card technologies, however, require a much more expensive reader. The laser card that was mentioned

earlier—a reader for that device that I had viewed some time ago was over ten times as much as it would cost to have done that with a smart card.

Senator KYL. Given that we are concerned here about quickly getting something in place that will work as best as we can make it work, and efficiencies are important here—we don't want to break the bank on it—are you saying that we could quickly put together a relatively inexpensive system that has the multiple features to it and have readers available for that?

Mr. COLLIER. It can be done, yes, sir.

Chairman FEINSTEIN. Would that system be a smart card system? What would that system be?

Mr. COLLIER. That would be the cost issue, Senator. Smart card reader technology is much less expensive than, say, an optical card reader or a two-dimensional bar code card reader. For instance, the raw components to make a smart card reader are under $20. The raw components to make a two-dimensional bar code reader are under $500. The system, again, that I viewed as prototypical for a laser card was almost $4,000 and as big as two bread boxes.

The other thing is where it is going to go. I mean, if you are going to put it in a turnstile, it is very doable, doable tomorrow with smart card technology and fingerprints or hand geometry, or even iris scanning. The card is really the issue more than the biometric is.

Senator KYL. May I just say thank you? I have got to run right now. Thank you, all of you, for helping us out today.

Chairman FEINSTEIN. Thanks, Jon, very much.

Mr. DOONAN. As the ambassador pointed out this morning, the real key to protecting against terrorism is having the database that has known or suspected terrorists in it. The general public crossing the borders—you could identify them and validate that identity as they move. The terrorist portion is probably less than 1 percent of the actual people you are talking about.

So the real challenge is sharing intelligence information between national and international law enforcement agencies. Somebody mentioned that most of these people have been arrested or fingerprinted at some point. It is a matter of collecting the biometric, whether it is a facial photograph that can be reliably matched or a fingerprint, and building that database so that the agencies that have to access it can do it.

Mr. CAMAROTA. One thing I wanted to add real quickly is that it might be important as soon as possible to start gathering fingerprints on all visa applicants, and part of the reason to do that is simply the deterrent effect. If you are considering coming to the United States to do harm, you are probably going to be very reluctant to give us all your fingerprints, as well as your photo, and so forth. So that could be very useful even if every component of the system is not entirely in place immediately.

Mr. SPADORCIO. Madam Chairman, may I add one other quick thing?

Chairman FEINSTEIN. Yes, please, and then I am going to go to Senator Cantwell.

Mr. SPADORCIO. I think the wise decision is really not to look at this as a an either/or, either fingerprints or facial or other biomet-

ric standards. I think the reality is which biometric fits the situation best for what you are trying to accomplish. The technology is moving in a direction that ultimately we will have multiple biometrics that we will be using in smart card approaches or other types of environments. So I think it really is what is the best technology to solve a particular problem.

Chairman FEINSTEIN. And what do you advise is the best technology to solve our particular problem?

Mr. SPADORCIO. Well, I really think it is probably two-fold. I think facial does a real good job for surveillance where you can actually passively scan crowds and look and see if you find somebody that matches the database. Fingerprints are absolutely wonderful for quick confirmation and authentication. So they both serve a little bit of a different purpose there, and I think you would almost want to do it in combination because you have two different means you are trying to serve.

Chairman FEINSTEIN. And so you could do both of those in a smart card?

Mr. SPADORCIO. Not necessarily in a smart card. Airports could introduce facial recognition systems that scan the crowd that are entering the airport. That is one way to do that. The smart card would be a great application for fingerprints for entry in and out of systems to verify identity.

Chairman FEINSTEIN. Thank you.

Senator Cantwell?

Senator CANTWELL. Thank you, Madam Chair.

Just to follow up on that line of questioning, I think it is important to note that the State Department has the ability to require fingerprints now, but they don't, on a standard basis. So the question becomes implementing that system and then integrating the databases.

Madam Chairman, I think the most successful Fortune 500 companies in our country even focused on information systems would find this problem before us challenging, not so much from the technology perspective but from the policy perspective of creating a standard—and I want to get to that question for Mr. Collier in a second about how do you do that on an international basis because once we develop this, we are not just talking about us—and then the coordination and decisionmaking between these various agencies.

So I think our panelists are pointing out quite specifically how the technology exists. It is a matter of us making decisions and then creating what layers of the database we want to have accessed by various people.

If I could, Mr. Doonan, I wanted to ask you about your specific fingerprint technology. What law enforcement are you currently working with now on your—what clients are you working with now on your fingerprint system?

Mr. DOONAN. We have about 34 systems in North America. The largest is the State of California that has a database of nearly 14 million fingerprints. We have the seven Western States that are in a consortium to share data amongst themselves. We have the State of Texas, the State of Illinois, Michigan, Virginia, Georgia, Pennsylvania. We have municipal systems throughout the country that all

interact with the State that they are resident in. Virtually all of our State systems interact with IAFIS to send the electronic fingerprint record of an arrested person or an applicant to the FBI.

Senator CANTWELL. Are you involved with driver's license records or not?

Mr. DOONAN. Actually, we are doing some preliminary testing of drivers' records.

Senator Feinstein, you seemed a little shocked that people would collect biometrics and not use them. Unfortunately, the State of California has about 30 million fingerprints that they collect for all their drivers, but they are never matched against anything.

Senator CANTWELL. What is your technology called?

Mr. DOONAN. The Automated Fingerprint Identification System. It basically matches the unique characteristics of the fingerprint against a database of any size.

Senator CANTWELL. And you have a patent of that technology?

Mr. DOONAN. Our technology. All of the AFIS vendors, their technology is proprietary, the actual matching algorithm. The interoperability between systems is achieved by utilizing what is called a NIST standard, the National Institute of Standards and Technology. We transmit image data that has been pre-defined in a standard format so that the different vendors can read and access their own databases on an image basis.

Senator CANTWELL. And only you have access to that algorithm, only NEC, or do NEC customers have access?

Mr. DOONAN. NEC customers use our algorithm to do the matching.

Senator CANTWELL. But I mean the code, the source code.

Mr. DOONAN. The source code is an NEC proprietary, just like it is for any other AFIS vendor.

Senator CANTWELL. Mr. Collier, you represent a group of businesses who are involved, but you are also a member of the consortium which has NIST and others involved, is that correct?

Mr. COLLIER. Correct.

Senator CANTWELL. And they are trying to establish this standard, somewhat like the W3C or IETF would come up with a standard that the industry can optimize around or use as a standard to build their various platforms. Is that right?

Mr. COLLIER. Yes. We have been engaged in standards development for some time, but it should be noted that the biometric industry has done a phenomenal job in putting together a consensus to arrive at standards both for exchange and interoperability of data.

We have currently the standard I mentioned earlier known as CBEFF, which is the Common Biometric Exchange File Format; the Bio API, which is primarily geared to the computer industry, which was one reason I think the biometric industry was motivated to move forward quickly because you can't play in that arena without standards.

X–984 is our current ANSI standard for fingerprints, and you did mention a minute ago about how does that roll into an international standard. That is actually being taken to the International Standards Organization, ISO, at this time. That governs all of our

bank cards and how biometrics would be stored on a credit card or an ATM card.

Senator CANTWELL. But ISO is only focusing on private sector adoption, or is there a government involvement?

Mr. COLLIER. There are government standards and guidelines, Senator, that are adopted by both commercial and government entities. NIST is an umbrella organization for the development of those standards. B10.8, which is another ANSI standard, affects drivers' licenses and credential-type applications. That, too, will move to an ISO standard. So the United States is leading the world in establishing international standards.

Senator CANTWELL. My question was about the international organizations. How do we get support from the Canadian government and others? Our system will only be as good as the protection that our allies will also give us, and while we are having lots of discussions with them on cooperation in our battles overseas, I think we should be having discussions with them about our cooperation on our various visa programs so that someone doesn't, like in the Ressam case, enter into Canada and then create more falsified information and enter the United States.

So is there a successful forum right now for that international dialogue as it relates to governments? Do we need to charge someone here within the administration to make sure that that dialogue is elevated to the level that it needs to be?

Mr. COLLIER. I think the best place for that to take place would be at the Biometric Consortium of the U.S. Government, which is led by the National Security Agency and the National Institute for Standards and Technology. They have been at this the longest and they have established cooperative efforts with other similar bodies overseas in the European Union as well as Asia. I don't know if the creation of a separate entity specifically aimed at standards would be necessary.

Senator CANTWELL. My question is how do we make sure that this gets elevated to the level—I am glad to hear that you think that we are having success there, so I would take it that you mean you think we are getting European cooperation.

Mr. COLLIER. Certainly, the groundwork have been laid for that and several meetings have been held for that. The Biometric Foundation and the International Biometric Industry Association also foster these relationships with other standards bodies overseas.

I think the change of importance of biometrics moving forward quickly with relevance to international standards is here on the front burner now. The activities of the agencies and organizations and institutions that I named have been terribly underfunded, with little or no funding for the past 10 years.

If they are expected to accelerate their pace and to bring about a consensus and that is going to require them to bear the burden of the expense of doing that, then that might be helpful as something that the Government could do.

Senator CANTWELL. Thank you. I see my time is up.

Chairman FEINSTEIN. Thanks, Senator.

Mr. Doonan, one of the most helpful things we have, I think, is this because I can actually understand it, this application process for biometrics-enabled passports and visas. You have one which is

a central database of known or suspected terrorists, and you have one that is a passport/visa management database. Then you have the non-biometric-enabled passport with a central database of known or suspected terrorists.

Does all of that get entered into one database, or do they remain as discreet databases?

Mr. DOONAN. Well, the known terrorist database typically would probably be a relatively small database; we are thinking 250,000 to 500,000. When a person applies for a visa or a passport, that fingerprint would be searched against that database to see if they enrolled. If they are enrolled, of course, you are not going to issue—

Chairman FEINSTEIN. And that would have intelligence information, as well as criminal records?

Mr. DOONAN. Yes. It may not have a fingerprint. It may have intelligence information that the ambassador spoke about.

Chairman FEINSTEIN. Right.

Mr. DOONAN. But it would be one database that national and international agencies could register data to. If the person applied and you identified them in some fashion, or suspected you identified them, you, of course, would not issue the document and you would notify the appropriate authorities.

If you did not identify them, you would enroll them then not in the terrorist database, but in a management database that then would allow you to manage—once the visa is issued, you would be able to manage the time frame that the person is supposed to be in the country. You would be able to scan their fingerprint when they left the country to know that they were out of the country.

For the student visa program, we would suggest a Web-enabled, inexpensive capability for the institution to be able to take a fingerprint when a person enrolled and confirm to that database that, in fact, they are a student enrolled in a university in the United States.

So the real problem is establishing a database of known terrorists and then establishing or moving from our current legacy system, where there is no biometric associated with millions of documents, and over time changing that so that we actually know who is in the country and we know that, in fact, the person holding that passport and that visa is who they say they are and the document was issued under the proper authority.

Chairman FEINSTEIN. Well, that is very interesting and it appears to be very doable.

Mr. DOONAN. It is quite doable.

Chairman FEINSTEIN. If you or any company were to come in and say we can do this for you, Federal Government, for all your agencies, what would be the length of time it would take to get that database, particularly with respect to terrorists, which is what we are interested in?

Mr. DOONAN. Of course, not being in the intelligence community, it is hard for me to say, but certainly we would work with all those agencies.

Chairman FEINSTEIN. Take your field, which is about 250,000, let's say.

Mr. DOONAN. Well, establishing the database shouldn't take a few months, I wouldn't think. Identifying the data to put in the

database should not be that difficult. The total implementation of this system and the maintenance system literally is a project that would never stop because you have to transition from a current situation where none of our documents are biometrically-enabled. And if you have 20 million or 25 million documents, through the normal attrition process or renewal process it would take years to actually do it.

But I don't think you have to look at that as something that is taking too long because if you establish the database and focus on the visa program, where the problem seems to be, I think a system could be operational and contain most of the problem literally within months or a little over a year, a few years, something like that.

Chairman FEINSTEIN. And you would use the systems that exist—IDENT, IAFIS, all of the other systems that are being put in place?

Mr. DOONAN. No, I would probably not recommend trying to do that. These systems are too large. They serve a different function. They are not anti-terrorist systems. They are large-scale identification systems. The interface between them is certainly something that is desirable, but I don't truly know how doable that would be.

Chairman FEINSTEIN. Truly what?

Mr. DOONAN. I don't know how doable that would be.

Chairman FEINSTEIN. In other words, these stovepipes that people spoke about, you don't think they could interrelate? Is that what you are saying?

Mr. DOONAN. Well, I don't have any specific information about those stovepipes. I am just saying that building a system like that and having that full integration is going to be a very difficult task.

Chairman FEINSTEIN. So it is easier to begin just with an identifiable system aimed at getting at this world of terrorism and who might be associated with that world?

Mr. DOONAN. Focus on the problem; that is, the terrorist problem.

Chairman FEINSTEIN. Now, just for that system, do you have any sense of cost?

Mr. DOONAN. Well, again, the database—

Chairman FEINSTEIN. Unless, of course, NEC, like Oracle, wants to do it for nothing.

[Laughter.]

Mr. DOONAN. Where is Larry Ellison when you need him?

The FBI system was $400 million. Somebody earlier said $40 million. It was actually $400 million.

Chairman FEINSTEIN. I said that. I had the wrong information. Thank you.

Mr. DOONAN. Again, the real problem is the number of times you have to search that database. Quite honestly, the biggest problem is the visa waiver program, the number of people that are coming into the United States that have not pre-applied for a visa, to have that searched against the database.

Again, I mentioned earlier the $500 million that Senator Bond had quoted. I would not quarrel with that number at all. It could easily be that, or more, but it would work.

Chairman FEINSTEIN. Thank you.

Does anyone have a last comment? I have found this very illuminating in a number of different respects, and very helpful. I think we know where we have to go.

Mr. DOONAN. Well, simply, NEC would like to thank yourself and the members for giving us the opportunity to speak with you. We are committed to the technology, we are committed to our country and company. Again, I would like to repeat the offer that if you would like us to bring an operational system here, it doesn't take a lot of room and we would be happy to bring it in and demonstrate that the technology does currently exist for yourselves, members and your staff.

Chairman FEINSTEIN. Well, I would like to take you up on that offer.

Mr. DOONAN. We will follow up with your staff.

Chairman FEINSTEIN. We will set something up.

Thank you all very, very much. Thank you for coming. The testimony has been excellent.

Thank you, ladies and gentlemen, for your attention.

The hearing is adjourned.

[Whereupon, at 1:00 p.m., the subcommittee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

Statement of Ted Goode, Director of Services for International Students and Scholars, University of California at Berkeley, Berkeley, California

All schools approved to issue I–20's are aware of the regulatory and statutory requirements to collect and maintain information on foreign students as specified in the regulations. Reporting to INS has been and remains an expectation by schools. The interface between schools and INS to accomplish the transfer of information has changed over the years. In the '70's schools sent to the local INS office a part of the I–20 document (a small card) to report a student's end of program. In the '80's INS was instructed to collect and maintain a larger amount of information on each student and in response created a computer based information system. INS collected the required information at the time of arrival in the U.S. and entered the information in a database. Schools were asked to review, verify and/or correct a report of students at that school prepared by and returned to INS. INS soon concluded that the system was neither efficient nor effective. The SEVIS electronic information system is the most recent attempt by INS to construct a system to collect and maintain required information. Schools have been prepared and remain prepared to be a partner with government to facilitate implementation of an efficient, effective and useful information system. Using the capability of current technology is clearly the way this objective should be met. A carefully crafted system that provides timely and accurate information is of interest to both schools and government. To ensure the success of such a system it must be user friendly for schools and government, usable across all computer platforms, and it must be reliable. I am confident that SEVIS can be crafted into this type of system through a close partnership between schools and government. The University of California supports Senator Feinstein's request to President Bush for the designation of 36.8 million to implement SEVIS. Appropriations to cover final development, implementation and maintenance must be sufficient to achieve this important goal.

The University of California appreciates your strong interest, support and leadership, Senator Feinstein, on this important issue. The University looks forward to the opportunity of close cooperation with you and your staff on this and other issues related to higher education.

Immigration and Naturalization Service, Department of Justice, Washington, DC, visa information on terrorist hijackers of September 11, 2001

The Immigration and Naturalization Service (1NS) compiled this information based on material provided by the FBI. Where applicable, known variations of common surnames were also checked. For some names (numbers 7 and 19 below), several name matches were found with different dates of birth, but INS was able to confirm admission as a nonimmigrant. In other cases (numbers 12 and 14-16), several name matches were found with different dates of birth, but INS was not able to confirm any information concerning those individuals.

(1) *Khalid Al-Midhar* was admitted to the United States as a nonimmigrant visitor in July, 2001. He appears to have been in lawful status on September 11, 2001.

(2) *Majed Moqed* was admitted as a nonimmigrant visitor in May, 2001. He appears to have been in lawful status on September 11, 2001.

(3) *Nawaq Alhamzi* was admitted to the United States as a nonimmigrant visitor in January, 2000. He appears to have overstayed the period of authorized time and was out of legal status on September 11, 2001.

(4) *Salem Alhamzi* was admitted as a nonimmigrant visitor in June, 2001. He appears to have been in lawful status on September 11, 2001.

(5) *Hani Hanjour* was admitted as a nonimmigrant student in December, 2000. We are unable to determine at this time whether this subject was in lawful status on September 11, 2001.

(6) *Satam A1 Suqami:* We are unable to find any record relating to this name

(7) *Waleed M. Alshehri* was admitted in June, 2000 as a nonimmigrant, and appears to have been in illegal status on September 11, 2001.

(8) *Wail Alshehri:* We are unable to find any record relating to this name,

(9) *Mohamed Atta* was admitted as a nonimmigrant visitor in July, 2001 and appears to have been in legal status on September 11, 2001.

(10) *Abdulaziz Alomari* is believed to have been admitted as a nonimmigrant visitor in June, 2001, He appears to have been in lawful status on September 11, 2001.

(11) *Marwan Al-Shehhi* was admitted as nonimmigrant visitor in May, 2001 and appears to have been in lawful status on September 11, 2001.

(12) *Fayez Ahmed:* We are unable to confirm any relating record based on current information available.

(13) *Ahmed Alghamdi* is believed to have been admitted as a nonimmigrant student and appears to have overstayed his authorized period of time in the United States before September 11, 2001.

(14) *Iiamza Alghamdi:* We are unable to confirm any relating record based on current information available.

(15) *Mohald Alshehri:* We are unable to confirm any relating record based on current information available.

(16) *Saeed Al ghamdi:* We are unable to confirm any relating record based on current information available.

(17) *Ahmed Alhaznawi* was admitted as a nonimmigrant visitor in June, 2001 and appears to have been in legal status on September 11, 2001.

(18) *Ahmed Alnami* was admitted as a nonimmigrant visitor in May, 2001 and appears to have been in legal status on September 11, 2001.

(19) *Ziad Jarrahi* was admitted to the United States as a nonimmigrant in July, 2001 and appears to have been in legal status on September 11, 2001.

Statement of Hon. Patrick J. Leahy, a U.S. Senator from the State of Vermont

I am pleased that Senator Feinstein is holding this hearing on a critical matter of concern. After the events of September 11, no one can doubt that we need to do a better job of preventing terrorists from entering our nation, and this hearing will provide valuable options for the Senate to consider. I would like to thank all of our witnesses for their testimony today. In particular, I would like to welcome Commissioner Ziglar, who has certainly endured a baptism by fire over the last month.

First, I would like to point out that one of the major security issues we face involves our border with Canada. The USA Act, the bipartisan anti-terrorism legislation that I co-sponsored and the Senate approved Thursday night by a vote of 96–1, includes important provisions that protect the chronically understaffed northern

border. While the number of border patrol agents along the southern border has increased over the last few years to more than 8,000, the number at the northern border has remained the same as a decade ago at 300. This remains true despite the fact that Admad Ressam, the Algerian who planned to blow up the Los Angeles International Airport in 1999, and who has been linked to those involved in the September 11 attacks, chose to enter the United States at our northern border. It will remain an inviting target until we dramatically improve our security.

The USA Act triples the number of Border Patrol, INS inspectors, and Customs Service employees in each of the States along the 4,000-mile northern border. I was gratified when 22 Senators—Democrats and Republicans—wrote to the President supporting such an increase, and I am pleased that the Administration agreed that this critical law enforcement improvement should be included in the bill. Senators Cantwell and Schumer in the Committee and Senators Murray and Dorgan have been especially strong advocates of these provisions and I thank them for their leadership. Now more than ever, we must patrol our border vigilantly and prevent those who wish America harm from gaining entry. At the same time, we must work with the Canadians to allow speedy crossing to legitimate visitors and foster the continued growth of trade that benefits both countries.

Beyond increasing security at our northern border, we need to take additional steps to protect our country. For example, we need to enhance information sharing between our intelligence agencies and the agencies that determine who gets into the United States—the State Department and the INS. The USA Act gives the State Department and INS access to the FBI's National Crime Information Center database, but we must go further to enhance the sharing of information from other agencies.

We also must make sure we develop the best possible biometric technology to identify potential terrorists entering the United States, such as facial recognition or fingerprint systems. The USA Act includes a section requested by Senator Cantwell that requires the Attorney General to report to Congress on the feasibility of enhancing FBI's Integrated Automated Fingerprint Identification System and other identification systems to better identify people with foreign passports or visas who may be wanted in connection with criminal investigations in the US or abroad.

In short, we need to examine the methods the State Department and the INS use to prevent terrorists from entering the United States, and provide those agencies with the enhanced resources they may need. We should also remember that although we need to call those agencies to make necessary improvements, they cannot bear all of the burden. To prevent future terrorist attacks, we must improve our intelligence-gathering capabilities, and make sure that intelligence about potential terrorists is shared with necessary actors throughout the government.

I am glad that Senator Feinstein is shedding light on these issues through this hearing, and I am very interested in hearing the testimony of today's witnesses.

ORACLE CORPORATION
REDWOOD SHORES, CA,
October 11, 2001

The Honorable Diane Feinstein
United States Senate
Washington, DC 20005

Dear Dianne:

It was great to see you see you yesterday. I enjoyed our conversation about a voluntary national ID system and the way different government agencies can share information to better protect our national security.

Oracle takes seriously our responsibility in these difficult times. As we discussed, Oracle is prepared to provide, free of charge, the Oracle software licenses for both testing and production of a complete national identification database.

I look forward to staying in close contact with you on these and other ideas as we all work to recover from the horrifying events of last month

Sincerely,

LARRY ELLISON
Chairman and Chief Executive Officer

○