S. HRG. 107–657

BIOMETRIC IDENTIFIERS AND THE MODERN FACE OF TERROR: NEW TECHNOLOGIES IN THE GLOBAL WAR ON TERRORISM

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

NOVEMBER 14, 2001

Serial No. J–107–46A

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
81–678 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, *Chairperson*

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

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

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

BIOMETRIC IDENTIFIERS AND THE MODERN FACE OF TERROR: NEW TECHNOLOGIES IN THE GLOBAL WAR ON TERRORISM

WEDNESDAY, NOVEMBER 14, 2001

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

Subcommittee on Technology, Terrorism, and Government Information, of the Committee on the Judiciary, Washington, D.C.

The Subcommittee met, pursuant to notice, at 10:05 a.m., in Room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein, Chairman of the Subcommittee, presiding.

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

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

Chairperson FEINSTEIN. I would like to call the meeting to order and welcome the witnesses, as well as the general public, to this hearing of the Subcommittee on Technology and Terrorism with respect to biometrics. That is the subject for this morning's panel.

I would like to welcome the distinguished ranking member, Senator Kyl from Arizona, with whom I have had the great privilege of working now for a number of years. And I might just say that we feel very similarly on these issues so I think it makes for a good working team.

After the September 11 attacks many Americans began to wonder how the hijackers were able to succeed in their plans. How could a large group of coordinated terrorists operate for more than a year in the United States without being detected and then get on four different airliners in a single morning without being stopped? The answer to this question is that we could not identify them. We did not know they were here. Only if we can identify terrorists planning attacks on the United States do we have a chance of stopping them. And the biometrics technology, the state-of-the-art technology of today, really offers us a very new way to identify potential terrorists.

Now it is true that biometrics would not deter suicide bombers who law enforcement and intelligence officials did not know about. However, it would make it easier to prevent entry by individuals who are known, who are suspected and who might try to hide their identity. For example, in the case of at least two of the hijackers, authorities had pictures of them as suspects prior to the attack and

airport cameras actually photographed them but because these cameras did not use facial biometric systems, security was not alerted and the hijackers remained free to carry out their bloody plans.

We also know that a number of the hijackers easily secured false ID cards, cards that they used to disguise their identities. If we had biometric devices in place these attempts may well—we cannot say for sure, but had a chance of being stopped.

Many experts believe that if we had been using biometrics for visa applicants and visa-holders and at customs, baggage and passenger checkpoints at airports, we could have potentially forestalled the September 11 attack.

One reason for this hearing is to explore the types of biometrics out there and how they can be used by government in conjunction with existing infrastructure and databases to prevent such attacks. I am concerned about just passing legislation mandating that the government use biometric technology because we all know horror stories about mandates going awry.

A month ago this Subcommittee heard from Paul Collier, the executive director of the Biometrics Foundation, who pointed out that the United States has issued 11 million driver's licenses and 5 million border crossing cards with biometric data but, and I quote, "There are no systems in place to read the biometric data and authenticate the cardholders." The point is that despite the fact that we have these systems, the departments have not put in place the readers. Consequently, the systems are wasted.

So 16 million smartcards have been effectively rendered dumbcards by lack of readers. Thus any biometric solution needs to be comprehensive and it needs to work.

Now what is biometrics? Biometric identifiers use unique biological information from people. It is fingerprints, it is facial structure, it is hand shape, it is the characteristics in the iris in our eye. These characteristics, measured, ensure that the bearer of the card is who they say they are.

So a biometric identifier is something that you are, a password or a PIN is something that you know, and a key or smartcard is something that you have. Biometric identifiers are the most secure and convenient way to authenticate and identify people because they cannot be borrowed, stolen, forgotten or forged.

I myself went to a street in Los Angeles, Alvarado Street, a while back and saw people literally by the dozens purchasing fraudulent Social Security cards, fraudulent driver's licenses, fraudulent other IDs. I saw where they print them and they did a beautiful fraudulent copy in less than 20 minutes and for anywhere from $15 to $150 a copy.

Biometrics make authentication relevant and positive. If you take a typical driver's license, which lists a person's eye color—blue, brown, green, maybe hazel, black—hundreds of millions of other individuals share that basic eye color. If you compare iris recognition technology, which also looks at the colored portion of a person's eye, the iris, this technology can identify around 270 unique characteristics of a person's iris and turn these characteristics into a code unique to that individual. So only one person alive

and only one person who had ever lived would have that code and that code could easily be put on a driver's license.

Many people assume that biometrics is something out of a high-tech action movie, a fancy expensive gadget with only few specialized uses. But, in fact, biometrics has begun to catch on, is becoming more and more widespread and is getting cheaper every day. In fact, there are $20 biometric devices you buy today to attach to your home computer.

So generally, biometrics can be used in three possible ways. It can be used to screen employees and control access to sensitive areas. This obviously prevents terrorists from getting a job as an airline or airport employee or posing as one in order to get access to implement a hijacking. A recent GAO audit found that inspectors were able to carry weapons around two airport security checkpoints merely by flashing false credentials. Such technology is already being used at places such as San Francisco International, Chicago O'Hare and Charlotte Douglas Airport.

Secondly, biometrics can be used to compare to a biometric database of criminals or terrorists to try to catch and stop them. So a terrorist whose picture or fingerprint is in a law enforcement database can be stopped before boarding a plane or entering the country.

Now this kind of biometric use is only as good as the database it uses. British law enforcement, as well as in Keflavik Airport in Iceland, uses this kind of biometric technology and currently the FAA is working on a computer-assisted passenger prescreening system, a system designed to use the passenger information system in airline databases to determine if an individual poses a security risk. So this system would be made infinitely more useful with biometrics.

Now I have received a number of phone calls from experts on biometrics and these experts, including the main biometric industry associations and the National Security Agency, have suggested that the industry is extremely fragmented, lacks minimal standards, and does not work well together, given the hypercompetitiveness of the companies. Currently, for example, there are about 140 companies trying to sell hundreds of different overlapping biometric devices of multiple types. These include fingerprints, hands, irises, faces, retinas, voice, handwriting, et cetera.

Now these companies are today aggressively marketing their different projects and they are criticizing their competitors. There is a lot of confusion about how best biometrics can be used in the war on terrorism. But experts are afraid that if government does not get involved to provide some order and structure, some standards if you will, then the market will result in a gradual and uneven adoption of biometric identifiers that will continue to leave our country vulnerable to terrorist attack.

There is no doubt in my mind that piecemeal adoption of biometrics can be a disaster. For example, the United States has issued these 16 million smartcards but there are no systems in place to read them.

I am looking, and I have suggested to the ranking member and Senator DeWine, who is here today, that we should also explore the creation of an unbiased center, a central clearinghouse if you will,

that can test, evaluate and set these standards for biometric solutions. The center would be a federally chartered nonprofit, tax-exempt corporation charged with mobilizing both government and the private sector to achieve today's most vital national security goal—helping to stop terrorism. The center would involve both the government and the private sector to be able to advise on how to choose and deploy biometric solutions that help detect and deter terrorists.

The center would involve the leading private sector biometric institutions. These would include the International Biometric Industry Association, the Biometric Foundation, the Center for Identification Technology Research at West Virginia University, the leading university biometrics center. The National Security Agency would be the initial coordinating agency for this center and could, at the president's discretion, be replaced by the Office of Homeland Security.

In the bill that Senator Kyl and I have been doing that Senators Kennedy and Brownback have just accepted into the bioterrorism legislation, we mandate that the centralized database—actually it is in the immigration bill—the centralized database be under the jurisdiction of the director of homeland security, just to avoid some of these problems, but the center would work closely with the Biometric Management Office at the Department of Defense, which has been chartered and funded to provide advice about military uses of biometrics to all defense agencies.

Of course there are many precedents for such a federally chartered center. The major one, of course, is the Manhattan Project, which enabled the United States to build the atomic bomb.

So this is an idea because I am getting very concerned about the conflicting information we have received. Today we have two government witnesses that I will introduce directly following my colleagues' remarks and then a panel of individual companies who are cutting edge companies that have come forward with some interesting biometric technology and they will be speaking about that technology and they have demonstrations which you will see scattered around the room that they will share their technology on.

Now I would like to recognize the very distinguished ranking member of this Committee, Senator Kyl.

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

Senator KYL. Thank you very much, Madam Chairman. I think the statement that you have just made summarizes my views and as a result I am just going to make one quick point and then get on with our witnesses. I know both of us have an obligation at noon and so the less you hear from me and the more we hear from you, the better.

We have been at this now for over seven years talking about the threats to our society, before those threats materialized, talking about the use of technology and it is comforting to me now at least to see a lot of colleagues and others saying, "You know what? We could use technology in this battle against terrorism."

So the purpose of this hearing this morning is not only to validate that point but to answer a couple of very specific questions

from experts. How specifically can we use technology, especially biometrics, to prevent terrorism, including illegal entry into the United States? And what do our governmental agencies need by way of legal authority or financial support in order to achieve these objectives in a very quick fashion? Those are the two questions I have. So to the extent you can get directly to those points in your testimony, I would appreciate it very much and I will simply put other remarks in the record, Madam Chairman.

Chairperson FEINSTEIN. Thanks very much, Senator Kyl. Senator DeWine, do you have comments you would like to make?

Senator DEWINE. No. I am anxious to get to the hearing and I just want to thank you, Madam Chairman, for having the hearing.

Chairperson FEINSTEIN. Thank you very much.

Then we will proceed with the first panel. I will just quickly introduce both witnesses and then they will proceed and hopefully limit their comments so that we can ask some questions back and forth.

The first is Michael Kirkpatrick of the FBI. Mr. Kirkpatrick is a 23-year FBI veteran, currently serves as assistant director of the Criminal Justice Information Services Division of the FBI. This division is the largest within the FBI. It was established in 1992 to serve as the focal point and central repository for criminal justice information services in the agency.

We also have Mr. Monte Belger with the FAA. He began his FAA career 28 years ago as an entry-level security inspector. He now serves as the acting deputy administrator of the FAA. He assists the administrator in leading a 49,000-person agency responsible for the U.S. aviation system.

Mr. Kirkpatrick, we will begin with you.

STATEMENT OF MICHAEL KIRKPATRICK, ASSISTANT DIRECTOR, CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. KIRKPATRICK. Good morning, Madam Chairwoman and members of the Committee, and thank you for the opportunity to appear before the Committee.

At the Criminal Justice Information Services Division of the FBI our mission is to reduce criminal activity by maximizing the ability to provide timely and relevant criminal justice information throughout the criminal justice community and to other appropriate agencies. The Congress and the taxpayers have invested almost $1 billion for the development and implementation of the sophisticated national computer systems housed at our West Virginia complex. Among the programs that we operate there of particular interest to the Committee this morning is our automated fingerprint identification program.

The FBI has served as the nation's fingerprint repository since 1924. During the first 75 years of that stewardship this was a manual, very labor-intensive process taking weeks and oftentimes months to process a single fingerprint card. With the full support of Congress and recognizing the need to significantly improve this critical service, the FBI, with our partners in the criminal justice community and with our partners in private industry, primarily Lockheed Martin, Planning Research Corporation and Science Ap-

plications International Corporation, were able to develop and build the Integrated Automated Fingerprint Identification System or IAFIS which became operational in July of 1999. The IAFIS provides the FBI with the ability to process key biometric fingerprints in a totally electronic environment and we do this 24 hours a day, seven days a week, 365 days a year.

Today we have approximately 42,800,000 digitized criminal fingerprint records in our database, which is by far the world's largest biometric repository of any kind. It is at least four times larger than all the fingerprint repositories in Europe combined.

Using this state-of-the-art technology we are able to process incoming electronic criminal fingerprints within two hours of their receipt and within 24 hours for in-coming electronic civil or applicant fingerprint submissions.

The IAFIS is a high-volume system with a capacity for growth. Last fiscal year we processed over 15 million fingerprint submissions, which equals about 1.3 million per month. Each day we add over 7,800 new criminal entries which are fully electronic-searchable to this database.

In addition to the tenprint capabilities of IAFIS, it also has a significant latent or crime scene fingerprint capability. When a latent fingerprint is lifted from a crime scene it can be sent in and searched against IAFIS, against the entire 42.8 million fingerprint records. Using this technique, cold cases which are decades old are being solved today which never were before. Since the inception of this capability, the FBI's laboratory has made over 700 latent identifications, which was more than the combined total in the prior 15 years.

On October 29 the president signed into law the USA Patriot Act. On behalf of the FBI I would personally like to thank you for the passage of this most important piece of anti-terrorism legislation. Pursuant to Section 405 of this law, the report on the Integrated Automated Fingerprint Identification System for ports of entry and overseas consular posts, I can report to you today that the FBI is already working closely with the Department of Justice and other federal agencies to prepare the report that was called for in the law on the feasibility of using the IAFIS to better identify individuals prior to their entry into the United States.

Since the IAFIS is the world's largest biometric database with an infrastructure which already connects local, state and federal agencies, it is a tool that could be used to move our country's security perimeter beyond our borders.

While the FBI believes that the IAFIS is a national asset, its development has also had significant international ramifications. On a global front, fingerprints are the most widely held and used forms of positive identification. In this regard the FBI has taken the lead in an effort to develop international standards for the electronic exchange of fingerprints. We frequently meet with our colleagues in the Royal Canadian Mounted Police and United Kingdom, as well as in Interpol, on this topic.

Technology for the capture, search, storage and transmission of fingerprints is widely available and, as you will hear today, becoming more economical. Fingerprint databases already exist at the federal, state and local levels and all existing criminal history

records are based on fingerprints. I invite the members of the Committee and their staffs to West Virginia to visit our complex and to witness firsthand this investment in state-of-the-art technology.

Again I thank you for the privilege of addressing this Committee and I am available to answer any questions that you may have.

[The prepared statement of Mr. Kirkpatrick follows:]

MICHAEL D. KIRKPATRICK, ASSISTANT DIRECTOR IN CHARGE, FEDERAL BUREAU OF INVESTIGATION, CRIMINAL JUSTICE INFORMATION SERVICES DIVISION

Good morning Madam Chairwoman and Members of the Committee. I am Michael D. Kirkpatrick, Assistant Director in Charge of the FBI'S Criminal Justice Information Services Division, or CJIS, and I Thank you for the opportunity to appear before this Committee.

I have served in the FBI for more than 23 years. In that time, I have served as a special agent in our Cleveland and Kansas City field divisions, and in various supervisory and management capacities in San Antonio, Texas; pocatello, idaho; and at FBI headquarters. In 1996, I was appointed as an Assistant Special Agent in charge of the New Orleans Field Division, where I oversaw investigations throughout the State of Louisiana. In August 1998, I was assigned to CJIS. Since my arrival in CJIS, I have served as the Chief of the Resources Management Section, and as the Deputy Assistant Director of the Policy, Administrative, and Liaison Branch. On April 4 of this year, the Attorney General approved my appointment as the Assistant Director in charge of CJIS.

CJIS was established in february 1992 and is the largest division within the FBI, with a current work force of 2,685. The division is located in Clarksburg, West Virginia, on a 986 acre campus. Construction of this world class facility started in October 1991 and was completed in July 1995, and I am proud to say on-time and under budget.

Our mission is to reduce criminal activity by maximizing the ability to provide timely and relevant criminal justice information to the criminal justice community and other appropriate agencies. The congress and the taxpayers have invested close to one billion dollars for the development and implementation of the sophisticated national computer systems housed at the West Virginia complex. Among the major programs managed and operated out of this division are: (1) the national crime information center, and (2) of interest to this committee today—the automated fingerprint identification program.

Since 1924, the FBI serves as the national fingerprint repository. For our first 75 years, the processing of incoming fingerprint cards was largely a manual, labor intensive process, taking weeks or sometimes months to process a single fingerprint card.

With the full support of congress and recognizing the dire need to significantly improve this critical service, the FBI, with our partners in the criminal justice community and leaders in private industry, including Lockheed Martin, Planning Research Corporation (PRC), and Science Applications International Corporation (SAIC), was able to develop and build the integrated Automated Fingerprint Identification System, or IAFIS. IAFIS became operational on July 28, 1999, and provides the FBI with a totally electronic environment in which to process fingerprint submissions 24/7/365. Today over 42.8 million digitized criminal fingerprint records reside in the IAFIS database, which is by far the world's largest biometric repository of any kind. It is at least four times larger than all of the fingerprint repositories in europe combined.

Using state-of-the art technology, the IAFIS receives, searches, and stores incoming fingerprint submissions, and generates responses within two hours of receipt for electronic criminal fingerprint submissions and within 24 hours for electronic civil submissions. IAFIS is a high volume system with a capacity for growth. In fiscal year 2001, our fingerprint receipts totaled 15,451,543 (7,991,125 criminal and 7,460,418 civil), which equates to 1.3 million receipts per month. Our FY 2001 receipts mark a six percent increase over those for the previous fiscal year. In addition, each day on average we add 7,853 new searchable criminal entries to this database.

At this point, I have only spoken about IAFIS's ten-print capabilities. This system can also process latent fingerprints collected as evidence of a crime. When a latent print is lifted from a crime scene, a latent fingerprint examiner can initiate a search of the entire IAFIS database to determine the suspect's identity. This technique has permitted the identification of criminal perpetrators from latent prints submitted from previously unsolved, "cold" cases. Since the inception of this latent search tech-

nique, the FBI's laboratory division has made 700 latent identifications using IAFIS technology. These 700 identifications are more than three times the total number of latent identifications made in the 15 years prior to IAFIS. These crimes would have otherwise been unsolved. This capability has had a tremendous impact on our public safety.

In response to the september 11 terrorists attacks, CJIS mobilized, along with the latent print units of the FBI's Laboratory Division, to provide disaster relief. This assistance included our "flyaway" interim distributed image system, or idis, terminals and remote latent fingerprint terminals. These computer systems allow disaster relief teams to submit both ten-print and latent fingerprints electronically to the IAFIS from remote locations. IDIS systems have also been deployed in other recent events, such as the summit of the Americas in Quebec.

Seven IDIS terminals, three latent work stations, and 32 CJIS employees were deployed to New York City; Dover, Delaware; and Shanksville, Pennsylvania, to Assist with Victim Identification. The New York disaster relief team reported 22 successful identifications, four using IDIS technology, and two using remote latent fingerprint technology. The Pennsylvania disaster relief team made one latent fingerprint identification.

On October 29, 2001, the president signed public law 107–56, the usa patriot act of 2001. On behalf of the FBI, I personally want to thank you for passage of this most important piece of anti-terrorism legislation. I can report that, pursuant to section 405 of this law, report on the integrated automated fingerprint identification system for ports of entry and overseas consular posts, the FBI is working closely with the department of justice and other federal agencies to prepare this report on the feasibility of using the IAFIS to better identify individuals prior to their entry into the united states. Since the IAFIS is the world's largest biometric database, with an infrastructure already connecting local, state, and federal agencies, it is a tool that could be used to move our country's security perimeter beyond our borders.

While the FBI believes that the IAFIS is a national asset, its development has had significant international ramifications. On a global front, fingerprints are the most widely held and used form of positive identification. In this regard, the FBI took the lead in an effort to develop an international standard for the electronic exchange of fingerprints. We frequently meet with our counterparts in the royal canadian mounted police and the united kingdom, as well as many representatives from interpol, on this topic. I am proud to say that international standards for the exchange and transmission of fingerprints, developed by the FBI, have been accepted by all member countries of interpol. We continue to have regular dialogue with our international partners in the rcmp, uk, and interpol on matters of mutual interest.

Technology for the capture, search, storage, and transmission of fingerprints is widely available and becoming more economical every day. Fingerprint databases already exist at the local, state, and federal levels, and all existing criminal history records are based on fingerprints. As I just stated, international standards have been accepted by all interpol member countries. These existing biometric systems form the foundation for coordinated domestic and international efforts and present opportunities to share information that can improve our national security and combat terrorism and trans-national crime.

I invite the members of this committee to visit the CJIS complex in Clarksburg and witness first-hand this investment in state-of-the-art technology. In closing, I again thank you for the privilege of addressing this committee. I am available to answer any questions the committee may have.

Chairperson FEINSTEIN. Thanks very much, Mr. Kirkpatrick.

The Ranking Member of the Full Committee has come, Senator Hatch, and I would like to recognize him and ask him if he has a statement he would like to make.

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

Senator HATCH. Thank you so much, Madam Chairman. I certainly appreciate it. I want to thank you and Senator Kyl personally for holding this important hearing and I also want to thank each of you for your steadfast resolve in helping to lead our nation's fight against terrorism.

Just recently your bipartisan support proved invaluable to our efforts to enact the USA Patriot Act of 2001, which provided much-

needed anti-terrorism tools to our law enforcement and intelligence communities. While the USA Patriot Act is a critical first step, more can and must be done to protect our nation from terrorists.

In particular, we need to tighten our border security, including our overseas embassies and consulates that function as our extended borders against terrorists. The Visa Entry Reform Act of 2001, recently introduced by the chairwoman, Senator Kyl and myself and others, will, by embracing new pioneering technologies, enhance our ability to prevent terrorists from ever setting foot in this country. As a proud cosponsor of this legislation I will help to see to it that it is passed into law.

The key to the legislation is its commitment to the use of biometric technology. Biometrics, the science of using physical characteristics to identify an individual, has long held promise in the areas of law enforcement and immigration. While individuals may be able to disguise their appearance sufficiently to fool the human eye, the technology we will hear described today can thwart the most sophisticated criminal mind.

One use for these technologies is in the immigration area where, by using biometric identifiers, we can conclusively confirm the identity of those seeking entry into the United States. Impersonation would be dramatically curtailed, if not eliminated all together. And in conjunction with law enforcement and intelligence databases, these technologies will enable us to identify potential terrorists before they are among us.

We had just yesterday a group call us claiming that they have a very low-cost iris identification system that may be very beneficial in these areas. We will be interested in following up on that, as we will with what every witness here is testifying to today, or at least the witnesses' testimony that we will receive today.

So I want to thank all of you witnesses who have agreed to come here to enlighten us and help us to know better what we should be doing in these areas and, above all, I want to compliment our chairwoman and ranking member for the leadership that they have provided against terrorism. And having lived through putting together the final anti-terrorism package that we have passed, an awful lot of that bill has been the work of this Subcommittee and the work of these two bipartisan senators who have worked so well together.

So I wanted to just personally come and congratulate them, thank them for the leadership they are providing, and tell them I am going to work very closely with them to make sure that what they do comes to fruition. And I want to thank each of you for helping us to do so. Thank you, Madam Chairwoman.

[The prepared statement of Senator Hatch follows.]

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

Madame Chairwoman, I want to thank you and Senator Kyl for holding this important hearing. I also want to thank the two of you for your steadfast resolve in helping lead our nation's fight against terrorism. Just recently, your bipartisan support proved invaluable to our efforts to enact the USA PATRIOT Act of 2001, which provided much-need antiterrorism tools to our law enforcement and intelligence communities.

While the USA PATRIOT Act is a critical first step, more can—and must—be done to protect our Nation from terrorists. In particular, we need to tighten our border security, including our overseas embassies and consulates that function as our

extended borders, against terrorists. The "Visa Entry Reform Act of 2001," recently introduced by the Chairwoman, Senator Kyl, myself and others, will, by embracing new pioneering new technologies, enhance our ability to prevent terrorists from ever setting foot in this country. As a proud cosponsor of this legislation, I will help see to it that it is passed into law.

The key to the legislation is its commitment to the use of biometric technology. Biometrics, the science of using physical characteristics to identify an individual, has long held promise in the areas of law enforcement and immigration. While individuals may be able to disguise their appearance sufficiently to fool the human eye, the technology we will hear described today can thwart the most sophisticated criminal mind.

One use for these technologies is in the immigration area, where by using biometric identifiers, we can conclusively confirm the identity of those seeking entry into the United States. Impersonation would be dramatically curtailed, if not eliminated altogether. And in conjunction with law enforcement and intelligence databases, these technologies will enable us to identify potential terrorists before they are among us.

Chairperson FEINSTEIN. Thanks very much, Senator Hatch. Your comments are very much appreciated. Thank you.

Now we will turn to Mr. Belger of the FAA.

STATEMENT OF MONTE BELGER, ACTING DEPUTY ADMINISTRATOR, FEDERAL AVIATION ADMINISTRATION

Mr. BELGER. Thank you. Madam Chairwoman, Senator Kyl, Senator Hatch and members of the Committee. I appreciate the opportunity this morning to represent the Federal Aviation Administration and talk briefly about the availability of modern security equipment and the development of future technologies, such as biometrics, for use at our nation's airports.

With the support of the Congress we have invested at the FAA over $440 million, every dollar that the Congress has provided over the past five years, to purchase and deploy explosive detection systems, explosive trace detection systems, threat image projection x-ray machines, and other technology. And in fiscal year 1902, this current fiscal year, we plan to spend an additional $293 million, the full production level, for explosive detection systems should we receive the president's funding request.

We are aggressively pursuing new technologies that can be deployed quickly. For example, in the area of explosive detection systems we have three vendors at our technical center who are developing a smaller version of explosive detection systems and we are working with them to develop and certify these systems as quickly as possible.

In response to one of the recommendations made by one of the two rapid response teams that were convened by Secretary Mineta, we have been working with both government and private sector technical experts to identify security technologies that are ready for deployment now, as well as those technologies that merit accelerated development.

As you suggested, Madam Chairwoman, we are getting involved and we are trying to bring some structure to these issues, at least as they pertain to application at airports, and I just want to mention three things that we have done in the past several weeks.

On October 25 we convened a subgroup of one of our security research and advisory Committees to evaluate the concepts in over 1,200 recommendations that have been made to the FAA. We have asked this group, which is both FAA and industry folks, for a re-

port of initial short-term recommendations by the end of this month and we have also asked that the advisory Committee provide a report to us to identify promising longer-term technologies.

Secondly, we are sponsoring what is now the third international aviation security technology symposium in Atlantic City later this month. This symposium will be important in helping to identify those technologies that can help meet the challenges we face. Right now we have over 40 vendors who will be present at this symposium later this month.

And thirdly, directly related to the biometrics issue for today, we have already formed an aviation security biometrics working group. This group is chaired by the FAA and the National Institute of Justice and we have brought together Federal agencies, both industry groups and law enforcement groups to develop a comprehensive concept of operations and application of some of these biometric systems in the aviation system and at our airports.

This group is particularly focusing on areas which biometrics can be used to improve aviation security and I think, Madam Chairwoman, the three issues I am going to mention are identical to the three that you mentioned that our group is focussing on. Those are employee identity verification protection of public areas through surveillance capabilities and passenger identity verification.

Biometrics that can be applied for purposes of passenger and employee identification include iris, hand geometry, fingerprint, voice, and facial recognition. And facial recognition also has the potential to be used for surveillance in public areas of airports.

Even before the September 11 attacks, some airports, a small number, but some airports, had started to test biometrics and integrate these systems into their security programs. For example, as you mentioned, San Francisco has been using hand geometry systems to control access to secured areas actually since 1992. Chicago O'Hare installed a pilot system for using fingerprint biometrics for increasing both the speed and the security checks for cargo truck deliveries at the airport. And Charlotte International Airport, in cooperation with U.S. Airways, tested a program in which iris recognition technology was used to verify employee identification before permitting access to secure areas.

The bottom line from the FAA is that biometric technology has the potential to improve aviation security and these systems are eligible for funding under the airport improvement program.

As we move ahead, I think we should keep in mind that there probably is no one solution, that probably technology by itself will not be the solution to the issues that we are facing, but these technologies hold great promise. As you also mentioned there are some significant challenges and in the world of aviation security we are anxious and willing and want to get involved to address these challenges and make these systems become operational at our nation's airports.

Our fundamental goal is 100 percent screening of all passengers, baggage, airport and airline personnel, and we believe that these systems have a role in the future.

So that concludes my remarks and I will be glad to answer any questions.

[The prepared statement of Mr. Belger follows:]

STATEMENT OF MONTE R. BELGER, ACTING DEPUTY ADMINISTRATOR OF THE FEDERAL AVIATION ADMINISTRATION

Chair Feinstein, Senator Kyl, Members of the Subcommittee:

I am pleased to appear before you today to discuss the availability of security related equipment and the status of the development of future technologies, in particular biometrics. In the aftermath of the tragedy that occurred on September 11, the Federal Aviation Administration (FAA), like the rest of the government, is rethinking our approach to security. The assumptions and strategies that were the basis of aviation security a few short weeks ago are being reassessed. No matter what overall direction and strategies we finally adopt, I want to assure you that the employees of the FAA continue to work tirelessly to identify and implement needed changes.

At the outset, I would like to discuss our most recent initiatives to ensure that all viable security technologies including biometrics, are being adequately considered, and that there is a plan in place to quickly take advantage of those promising technologies that can assist us in our fight against terrorism. In response to one of the recommendations made by the rapid response teams convened by Secretary Mineta in the aftermath of September 11, the FAA was tasked with working with both government and private sector technical experts to identify beneficial security technologies that are ready for deployment, as well as those technologies that merit accelerated development. We will identify technologies that we can deploy, both short term and long term, which can significantly augment the screening of passengers, checked luggage, cargo, and airport and airline employees.

The FAA's efforts to increase airport security since September 11 include the formation of the Aviation Security Biometrics Working Group. This working group, chaired by FAA and the Department of Justice's National Institute of Justice, has brought together representatives of Federal agencies, industry and law enforcement to develop a comprehensive concept of operations for the application of biometrics in aviation security.

The biometrics working group has identified four areas in which biometrics can be used to improve aviation security: (1) employee identity verification and access authorization to secured areas within an airport; (2) protection of public areas in and around airports through surveillance to prevent harm to airports and aircraft; (3) passenger protection and identity verification which would involve enrolling passengers in a national identification system, and likely to have multiple biometrics; and (4) aircrew identity verification both on the ground and en-route. Biometrics that can be applied for the purpose of passenger, employee and aircrew identification include iris, hand geometry, fingerprint, voice and facial recognition. Facial recognition has potential to enhance aviation security through surveillance, as the technology matures.

Prior to the September 11th attacks, airports had started to test the utility of biometrics for improving airport security, and integrating biometric systems into their security programs. For example, San Francisco International Airport has been using hand geometry systems to control access to secure areas since 1992. Chicago's O'Hare airport installed a pilot system using fingerprint biometrics for increasing speed and security for cargo truck deliveries at the airport. Also, Charlotte/Douglas International Airport, in cooperation with US Airways, conducted a pilot program in which iris recognition technology was used to verify employee identification before allowing access to secure areas. Additionally, the Immigration and Naturalization Service uses the INS Passenger Accelerated Service System (INSPASS), a hand geometry technology, at nine international airports to expedite frequent travelers' processing into the United States.

Biometric technology has the potential to greatly improve aviation security and is one of the most commonly recommended technologies for doing so. Although there are still questions regarding this promising technology and its effects on the privacy and civil rights of the American people, resolving these issues remains a priority for both Secretary Mineta and the Administrator. Of course, the new security measures have been and would continue to be implemented in a manner consistent with our commitment to protecting passenger and employee civil rights.

In addition to the biometrics working group initiative, on October 25, the FAA convened its security research and advisory committee, chaired by John Klinkenberg, Vice-President for Security for Northwest Airlines, to work toward achieving our security goals. This Committee will evaluate over 1,000 recommendations made to the FAA by various industry sources. The Administrator asked that the Committee provide her with a report on its initial recommendations by the end of November. The Administrator expects the report to identify the most promising technologies for providing early security benefits to the flying public, as well as their

suggested implementation strategies. Likewise, the report will identify promising longer term technologies that are worthy of accelerated development.

The FAA is also sponsoring its third International Aviation Security Technology Symposium in Atlantic City, New Jersey from November 27 through November 30. This symposium will feature numerous sessions on diverse security topics including human factors, deployment of new explosives detection equipment, emerging technologies, aircraft hardening initiatives, cargo screening, and integrated security systems. Attendees will have the opportunity to view, first hand, vendors' security technologies. The symposium, which is also sponsored by the National Safe Skies Alliance, Airports Council International, Air Transport Association, and the American Association of Airport Executives, was planned before the terrorist attacks, but it is now that much more critical for identifying those technologies that can help meet the challenges we face in this new era of heightened aviation security.

Now that I have provided an overview of some of our most recent security initiatives, I would also like to provide a broader overview of our efforts to enhance security through technology. The goal of aviation security is to prevent harm to passengers, crew and aircraft, as well as to support national security and counter-terrorism policy. How we achieve that goal now requires that we take a comprehensive look at how airport screening is undertaken from workforce, technology, and procedural standpoints. The Administration is looking at all options and has not ruled out any alternative at this time.

Four years ago, the White House Commission on Aviation Safety and Security (the Commission) issued 57 recommendations, the majority of which focused on improving aviation security. Most importantly, the Commission acknowledged that aviation security was a national issue that required a national focus and reliable funding. In the area of security technology, it was recommended that FAA deploy existing security technologies, establish standards for developing technologies, and work with other government agencies and industry to develop new technologies. Thanks to Congressional support of these recommendations, the FAA has spent $445 million in the past 5 years to purchase explosives detection systems (EDS), explosives trace detection (ETD) devices and threat image projection (TIP) ready x-ray machines. In fiscal year 2002, we plan to spend an additional $293 million, the full production level for EDS equipment, should we receive the President's funding requests.

One hundred fifty-nine EDS machines have been installed at airports across the country and we are working to deploy over 20 more in the coming months. In addition, we need to work with the companies that manufacture the systems to see how quickly they can produce more systems for continued deployment. Products of two EDS vendors have been certified and variations of these products are currently going through the certification process. Prior to September 11, EDS was primarily used to screen checked bags belonging to persons identified by the Computer Assisted Passenger Prescreening System (CAPPS). CAPPS allows the air carrier to focus EDS screening on a manageable number of passengers, for example, those whom we cannot discount as potential threats to civil aviation, based on parameters developed within the counter-terrorism community and reviewed by the Department of Justice to ensure that the methods of passenger selection do not result in illegal discrimination. CAPPS also selects passenger bags on a random basis for additional screening. In the aftermath of September 11, FAA has committed to increasing the number of passenger bags that are randomly screened. Furthermore, EDS machines are now running continuously at those airports to which they have been deployed, CAPPS has been adjusted and passengers and their carry-on items are being screened on a continuous basis at the boarding gate.

In addition to EDS, FAA is currently purchasing ETD devices from the three vendors with FAA approved products. These devices can detect the presence of explosive materials in a passenger's checked or carry-on bags. As of last Friday, we had installed 884 ETD devices in 177 airports across the country.

Another tool available to test and measure screener proficiency is software technology, known as the Threat Image Projection (TIP) system, installed on conventional x-ray machines. TIP electronically inserts images of possible threats (e.g., a gun, a knife, or an explosive device) on a x-ray monitor. The monitors show the image as if it were within a bag being screened. Its purpose is to provide training, keep screeners alert, and measure screener performance. High scores detecting TIP images equate to a high probability of detecting actual bombs and dangerous weapons. Not only can TIP data be potentially used to assess screener performance over time, but the results can also be used to analyze any correlation between performance and experience. New images will be added to the FAA-approved TIP library being installed on the x-ray machines at the security checkpoints to improve screen-

er vigilance and training. To date, 741 of these units have been deployed to 75 U.S. airports for checkpoint screening.

Aside from those technologies approved by the FAA, there are a variety of technologies in various stages of development. As is the case with other areas in which the FAA has regulatory oversight, FAA sets a security standard airlines and airports must meet. It is routine in the airline industry for individual carriers or airports to exceed FAA standards in certain areas and I think we need to look at how that approach might be incorporated with respect to aviation security.

Although, FAA does not currently require airports or airlines to have EDS, if they do have the equipment, we require them to use it. We will continue to work aggressively so that every screening checkpoint gets the equipment it needs to ensure a more effective aviation security system

We also need to determine whether other security technologies currently in development can be effectively used by airlines and airports. For example, there are a number of backscatter technologies, chem/bio trace detection, and portal screening technologies that are in different stages of development. As I mentioned earlier, biometrics (e.g., iris and finger print identification) are currently being tested in the operational environment. The Rapid Response Team on Airport Security also recommended that we should move to a greater use of positive identification technologies. We are considering this recommendation and we are working with industry to see whether and how all of these efforts can be incorporated into airline and airport operations to improve aviation security, while upholding America's steadfast commitment to the protection of civil rights. To this end, we have met and will continue to meet with civil rights groups to discuss how we can ensure continued protection of Americans' civil rights as we incorporate enhanced security measures, including some of the new technologies.

Just to make sure that we are not missing anything that is out there, FAA issued an announcement that appears on our web site (*www.faa.gov*) requesting information about any product or technology that could be helpful in improving aviation security. As you can imagine, this requires sorting through a great deal of information. So, while there does not appear to be a single technology that addresses all of our security concerns, we are committed to working through the various options available to us.

The Secretary of Transportation, the FAA Administrator and the entire Administration are doing everything in our power to bring the nation's air transportation system back into full operation with the highest levels of safety possible. Recently, Secretary Mineta directed FAA special agents to crack down on airport and air carrier security deficiencies by taking decisive steps, including clearing concourses, rescreening passengers, and even holding flights where appropriate. This action reflects both the Department's and the FAA's unyielding commitment to civil aviation security and the restoration of public confidence in the nation's air transportation system. It is clear that through constant vigilance, the application of new technologies and procedures, and assistance from its national and international partners, the FAA will succeed in its civil aviation security mission.

Because civil aviation exists in a dynamic environment, the FAA must develop a security system that optimizes the strengths of a number of different technologies. This system must be responsive to potential means of attack and must be able to anticipate future risk to the civil aviation environment. In a democracy, there is always a need to balance freedom and security. Our transportation systems, reflecting the value of our society, have always operated in an open and accessible manner, and we are working hard to ensure that they will do so again.

This concludes my prepared remarks. I would be happy to answer any questions you may have.

Chairperson FEINSTEIN. Thank you very much. We appreciate your comments.

I will ask two quick questions, the first one to Mr. Kirkpatrick.

In your view, which biometric would be the most effective against terrorists? And if you should indicate fingerprints, what do you say about the fact that we do not have fingerprints for many of our terrorists in the database and part of that question is were the fingerprints of any of the September 11 hijackers in an FBI database?

Mr. KIRKPATRICK. Madam Chairwoman, I think that as Mr. Belger said, there is no single biometric application that is going

to be the be-all-and-end-all. I think you have to look at the use that it would be put to.

Fingerprints would play a very important part in positively identifying someone and, along with a digital photograph or other biometric, enrolling them in a system and then possibly some other type of biometric hand geometry, iris recognition could be used to control access in and out of areas.

To my knowledge, there were none of the September 11 terrorists who were in the FBI fingerprint database, no.

Chairperson FEINSTEIN. Thank you very much.

And one for Mr. Belger. Can you tell me how many airports are submitting the fingerprints of their new employees for a criminal fingerprint check?

Mr. BELGER. Yes. Today and since December of last year the 21 airports, what we call the category X airports in this country, under legislation that was passed last year have been submitting fingerprint checks for all new employees who are working as passenger screeners or who are working in secured areas of the airport. We would like to extend that to all airports and we would like to extend it to all employees, not just those that are being hired now but all current employees. As the administrator said a couple of weeks ago, we are working on a rule to do that and I hope to be able to have that on the street very soon.

Chairperson FEINSTEIN. I think that is extraordinarily important in terms of saying to people that our airports are secure. How soon do you estimate that will be?

Mr. BELGER. We are talking days.

Chairperson FEINSTEIN. Days. And that will be for everybody—

Mr. BELGER. Yes, we would include—

Chairperson FEINSTEIN. —who works at an airport. It will go back even if—not just new employees.

Mr. BELGER. That is correct. We would like to ensure that every employee at every airport who is working as a screener or is involved in that process or who has access to the very sensitive and secured areas of the airport has gone through a criminal history records check, which requires a fingerprint.

Chairperson FEINSTEIN. Right. And can you tell us what biometric technologies the FAA is currently using?

Mr. BELGER. Well, the three airports I mentioned are using different systems. We are currently testing and evaluating the whole range of capabilities and we are trying, as you suggested, to bring some order in the form of a concept of operations of how these systems can most effectively be used at airports and that is where we are focusing right now. There is very little use today at our nation's airports of these biometric systems. We are trying as best we can, within the aviation world at least, to establish some operational concepts and some standards so that we can help our airports pick the right ones to use.

Chairperson FEINSTEIN. I have to ask one more quickly. Do you feel you are equipped to set the standards? I do not mean that in a derogatory sense. I mean there is just so much competition out there; it is very difficult.

Mr. BELGER. It is. I talked to one of the gentlemen this morning who is working on this full-time at our technical center up in At-

lantic City and he expressed that same thought. We are doing the best we can. I think we would be delighted to work with an organization, as you suggested, that would be charged with setting some national standards. We would be delighted to do that.

Chairperson FEINSTEIN. Thank you very much.

Senator Kyl?

Senator KYL. Thank you.

First Mr. Belger. You indicate that you are working hard to I prove the passenger manifest system, would like to make it mandatory, and that all airlines would be required to participate, and also to expand that to other types of travel—cruise lines and cross-border bus lines, and the like.

Is there any way that we can require all passenger manifest information prior to departure and boarding, rather than prior to arrival? And would it not make sense in trying to prevent terrorism to prevent the terrorists from actually boarding the actual mode of transportation? How could that all be done?

Mr. BELGER. If I could answer that perhaps in two ways, one, for passengers who are departing from the United States, we do have a system in the FAA or with the carriers where we do apply a preboard screening profiling system which is rather effective.

In terms of arriving passengers into the U.S., which I think was the first part of your question, that is really an INS and a Customs responsibility more so than the FAA's but your suggestion that it would be a good idea to know who is on that airplane before they get here is certainly a good one.

Senator KYL. It is my understanding that the fingerprint check for employees will soon be required for everyone having access to secured areas in airports. That includes people like food service people and the like, does it?

Mr. BELGER. Yes, sir. It would be anybody who has access to those areas.

Senator KYL. Now that system is only as good as the continued check of the identification of people who are coming in and we have evidence that there was on the person of some of the people that are being investigated in connection with the September 11 events forged documents for different airline personnel positions, some of which presumably would permit them entry into a secure area. You may determine that John Doe has no criminal background and therefore could be hired to work at the airport but if someone steals John Doe's identification or it is not a tamper-proof kind of identification, what is to prevent somebody from gaining unauthorized access today to a secure area?

Mr. BELGER. Those are vulnerabilities and we do require the airports who issue these identification cards to periodically inventory and check to make sure that the cards they have issued are, in fact, in the possession of the person they issued them to. So we do require them to periodically check their database and check the cards that they have issued to make sure that they are still in the hands of—

Senator KYL. But there is not any biometric identifier required today.

Mr. BELGER. That is correct.

Senator KYL. There is none today.

Mr. BELGER. That is correct.

Senator KYL. Would that not be a necessity, to have security?

Mr. BELGER. It would certainly help. No doubt about it; it would help to ensure that the person is the person who applied for and received that card. We are encouraging airports to go ahead and start using these systems. There is really nothing today that prevents an airport from—

Senator KYL. Well, I think leadership has to come from the top and it has to be—this is a matter of national security now. I do not think it is sufficient to simply say we have encouraged airports to figure out how to ensure the security of their own perimeters and of their own personnel.

We believe, I think, that there has to be a national standard applicable to all of the major airports and we believe that biometric technology is a way to ensure that the people who show up for work can be identified as the appropriate people. Should it not be FAA policy to develop that national system and try to put it into place as soon as possible?

Mr. BELGER. I believe it is and we are starting to do that. We are trying to do that. To the extent that there are other folks who are working on national standards, we would love to be a part of that.

Senator KYL. I think we will be sure you are part of it. One of the things that Senator Feinstein pointed out and she actually demonstrated this to the audience at the last hearing we had is that many federal documents like pilot licenses are not fraud-proof. They are, she pointed out, just a little cardboard with a perforated edge that you kind of tear out of a sheet and obviously there are other documents that permit a pilot to gain entry to secure areas but those are the kinds of documents that should have a biometric identifier, are they not, in your opinion?

Mr. BELGER. I think they should in the future, yes, sir.

Senator KYL. Mr. Kirkpatrick, do you agree with that?

Mr. KIRKPATRICK. Yes, sir. I would just add that I think that a criminal history check based upon fingerprints could serve as a strong foundation upon which the biometrically based access systems that you are referring to could be added on top of.

Senator KYL. Right. One of the things that—this will be my last question and it is directed to you. In response to Senator Feinstein's first question relating to the terrorists and not having fingerprints on them, and so on, you said basically all of these tools are useful in different ways for different functions. We all understand the need for a national fingerprint database to catch criminals here in it U.S. and identify people and the like, but it may not be the most useful with respect to preventing terrorists from other countries coming into our country.

What we need from you is testimony today and recommendations later about how to integrate those systems and how to prevent having too many duplicative systems to try to reduce the cost so that we have one way of looking at things hopefully over time. Any particular thought on that?

Mr. KIRKPATRICK. Well, my thought on that, sir, would be that we need to build upon the infrastructure that is already in place and have a greater integration of information that exists in various

different agencies' stovepipe-type systems today. I think that the attorney general and the director have both spoken very vocally about the need to share information better and I think that that would certainly fall underneath that.

Senator KYL. Thank you.

Chairperson FEINSTEIN. Senator DeWine?

Senator DEWINE. Madam Chairman, thank you very much.

Mr. Kirkpatrick, thank you for your testimony. You reference Section 405 of the Patriot Act, which is a provision that I wrote that you are now beginning to implement. I am glad to see that you are moving forward.

I wonder if you could give us some idea about what the FBI's concept is for applying this IAFIS system to the embassies. I am sure you have some idea. We are not asking for your report yet but maybe a little preview of what is possible there.

Mr. KIRKPATRICK. Yes, sir. And this is very preliminary in terms of—

Senator DEWINE. We will take it that way.

Mr. KIRKPATRICK. —the concept.

We believe that livescan fingerprint devices could be deployed out at the embassies and consulates to take 10 fingerprints and also capture a digital photograph of individuals who are applying for visas in their home countries. Those could then be transmitted to the FBI for a criminal check but in addition to that, and this would be a new developmental effort, a visa or visitor file could be developed in which these could then be stored. When the person arrives at our country at the airport or the seaport they could then put down one fingerprint, which could be used to verify that the person who the checks were done on prior to them coming to our country is, in fact, the person who shows up at our borders to enter the country.

Additionally, that could be expanded to use that one fingerprint to verify, upon their departure from the country, that this is, in fact, the same person leaving. It would give you some kind of an inventory of who is here and who is not.

Senator DEWINE. So you really have the potential for two, three different uses, at least, different functions, different tasks.

Mr. KIRKPATRICK. Yes, sir.

Senator DEWINE. Well, we wish you well. Thank you very much.

Mr. KIRKPATRICK. Thank you.

Senator DEWINE. Mr. Belger, let me ask, I do not quite understand the FAA's jurisdiction for airport security in regard to federal law enforcement and intelligence agencies. Who has what responsibility and how are you working together in light of the new world after September 11?

Mr. BELGER. Well, in terms of law enforcement and intelligence specifically, the FAA first of all is not an intelligence-gathering organization. We rely upon the FBI and others for intelligence information. We do have within the FAA security organization a very good sophisticated intelligence analysis capability. We work very closely with the FBI and the CIA and others and we actually have people assigned full-time to those agencies as liaisons. We are constantly in touch. We get information from them. We assess that, along with the intelligence agencies, for application for aviation

purposes and then if it is appropriate, send that information out to the airports and the air carriers for implementation.

Senator DEWINE. Has that relationship changed since September 11?

Mr. BELGER. Well, I think it has changed over the years. I think it is even better and closer than it was before September 11. We are constantly in touch to the extent that we have people at those intelligence agencies representing the FAA.

Senator DEWINE. You talked a little bit about the use of technology that electronically captures fingerprints for background checks and it is my understanding that airports in SEAttle, Los Angeles, Denver, Dallas–Fort Worth, JFK, Chicago use that technology to transmit into the database to do the background check.

What is the plan as far as expanding the program? Question for either one of you.

Mr. BELGER. I will answer in terms of expanding the requirement to other airports. Those large airports that you mentioned, they do, most of them, probably all of them, have electronic fingerprint transmission capability, which obviously speeds up the process. What used to take weeks now probably takes a day or two to get a reading back.

So as we had said earlier, we are in the process of putting together a requirement that would expand the requirement to do criminal history records checks to all airports. We are also making available under the airport improvement program funding for those electronic fingerprint machines for any airport to purchase should they want to.

Senator DEWINE. What kind of cost is that?

Mr. BELGER. I am not really sure what the cost is. I do not think they are real expensive but I honestly do not know, per machine, what the cost is.

Senator DEWINE. Thank you, Madam Chair.

Chairperson FEINSTEIN. Thank you, Senator.

Senator Cantwell, welcome.

Senator CANTWELL. Thank you, Madam Chair, and thank you for holding this important hearing. I know that your commitment and Senator Kyl's commitment to this very important issue is helping us put a shape and, if you will, face to what we need to do in biometrics.

I was very happy to get language added to the anti-terrorism bill that specifies that the Department of Justice and the Department of State should work together in adopting a biometrics standard to be used for the visa program and hopefully to be used by our allies abroad in also identifying people who want access to the United States. So I think this hearing is very helpful in talking about where we have been today on biometrics and how we can get that standard established.

Mr. Kirkpatrick, I appreciated your testimony. I wanted to ask a few questions about the IAFIS system and where you have been today because I think actually part of that technology is perhaps a company that is based in Washington State that is the basis for that. But your system is currently fingerprint only or are you already adding in facial recognition to the fingerprint system?

Mr. KIRKPATRICK. We have the capability to store photographs in that system. It is at this time not searchable by photograph. However, there is the capability to associate a photograph with a particular set of fingerprints.

Senator CANTWELL. Do you have any idea of how many records like that you have?

Mr. KIRKPATRICK. No, I do not.

Senator CANTWELL. Is it 10 percent or 15 percent?

Mr. KIRKPATRICK. I do not know, no.

Senator CANTWELL. Is the FBI at a point where it is recommending that the database should be a compilation of both facial recognition and fingerprints or have they made that determination?

Mr. KIRKPATRICK. We would like to have a photograph associated with every record. We have the capability to store that, as I said. We need to work with our partners in state and local and other federal law enforcement agencies to make sure that they have the capabilities to take those photographs and associate them with the records and forward them on to us.

Senator CANTWELL. Given your involvement on an international basis, and I believe that the IAFIS system is also the basis of what Interpol uses so we have gotten some international standards established here, at least as it relates to fingerprints; is that correct?

Mr. KIRKPATRICK. FBI fingerprint transmission standards have been adopted by Interpol, yes, ma'am.

Senator CANTWELL. And if we were going to go to the next level on a broader biometric standard using both facial recognition and fingerprints, how do you think we should best go about that?

Mr. KIRKPATRICK. Given that there are already international standards for fingerprints, I believe that we would have to have some type of a concerted international effort to allow the routine sharing of those. What we have found, working with some of our international partners, is that many times their privacy laws are much more restrictive in those countries than even here in the United States and that has precluded routine sharing of that.

So it is going to require, I believe, a fairly broad diplomatic effort to make that happen.

Senator CANTWELL. And given that you have been involved in that before, do you think that is the State Department?

Mr. KIRKPATRICK. We are trying to resolve that. In fact, we are very close with one of our international partners to being able to routinely exchange electronic fingerprint information with them. We are working with another very closely and are trying to work through the legalities of doing that. I am not sure at this point it is a State Department situation but it is certainly something that we would need to focus greater efforts on.

Senator CANTWELL. And is it your understanding—I think I saw in your testimony that all of the Interpol members have adopted that standard? Is that correct?

Mr. KIRKPATRICK. Interpol has adopted the FBI standard for electronic transmission of fingerprint information; yes, ma'am.

Senator CANTWELL. So what does that mean as far as the Middle East is concerned?

Mr. KIRKPATRICK. It would mean, and I think, as you will hear possibly later from some of the biometrics vendors, it means that,

for instance, fingerprint livescan machines are all developed according to this standard so that one company's fingerprint capture machine can, if you will, talk to another company's and that type of thing. It would mean that the fingerprints that are taken by another country electronically are in the same format as those here in the United States. It allows for a much easier sharing across countries of those fingerprints.

Senator CANTWELL. Thank you.

Thank you, Madam Chair. I see my time has expired.

Chairperson FEINSTEIN. Thank you very much, Senator.

Just a quick point of clarification, Mr. Belger. You mentioned that a rule is going to be published momentarily requiring all employees at airports to have a criminal background check. Are these just employees in secure areas or all employees? And secondly, how many employees will that cover?

Mr. BELGER. It would be employees in two categories. The first category would be people who are performing the passenger screening functions and supervisors and anybody related to that function. And the second category would be all employees who have unescorted access privileges to the secure areas of the airport. In other words, people who can be on the ramp or in the baggage make-up area, around airplanes, in those areas, before they, number one, could be employed and number two, within a certain time period, they would have to go through a criminal background check.

Chairperson FEINSTEIN. And how many people does this involve?

Mr. BELGER. We have estimates at this point but the number that I think we are most comfortable with right now is in the neighborhood of 700,000 people.

Chairperson FEINSTEIN. I see. And are airline personnel included?

Mr. BELGER. Yes, they are.

Chairperson FEINSTEIN. Thank you very much.

Well, we thank you both. You were very helpful. We really appreciate your being here this morning. Thank you so much.

Senator KYL. Senator Feinstein, I am going to have a series of written questions. Because we do want to complete the hearing before noon, we need to move to the next panel but I have a series of written questions that I would like to get both of you to respond to.

Mr. KIRKPATRICK. Yes, sir.

Senator KYL. Thank you very much.

Chairperson FEINSTEIN. Thank you and we will excuse these witnesses and ask the following—Dr. Atick, Joanna Lau, Valerie Lyons, Bill Willis, Martin Huddart, and Richard Haddock to please come forward.

I am going to, if it is all right with Senator Kyl, just proceed and introduce all of you at one time. Then we will begin and go right down the table with comments. I would ask you to keep your comments to five minutes so we will have an opportunity to ask questions.

I will begin on my right, the audience's left, with Valerie Lyons of Identix. She serves as executive vice president of world sales of Identix. She was formerly president of Cytel, a privately held e-

business infrastructure services firm. Identix is the leading developer of finger biometric systems and is and has already installed biometrics fingerprinting-based screening systems for job applicants in some of the nation's largest airlines and airports, including United, Continental, JFK, and Dulles International Airports.

Next is Mr. Bill Willis of Iridian Technologies. He joined Iridian as chief technology officer this year, brings more than 20 years of technology management. Iridian is the leading developer of authentication technologies based on iris recognition, which they claim is the most accurate biometric identifier.

Next is Dr. Joseph Atick of Visionics Corporation. He serves as chairman and CEO of Visionics, a company that produces facial recognition and fingerprint matching systems. Prior to founding Visionics he served at the Computational Neuroscience Laboratory at Rockefeller University and prior to that, the Neurocybernetics Group at the Institute for Advanced Studies in Princeton, New Jersey. He will testify on the benefits of facial and fingerprint biometrics and is therefore uniquely qualified to speak on the deployment and benefits of both products.

Martin Huddart of Recognition Systems serves as general manager of Recognition Systems. This company was founded in 1986. It specializes in the development of hand geometry biometric systems identifying people by the size and shape of their hand. The company has 55,000 units installed throughout the world and serves clients that includes private industries, law enforcement, and the Olympic Games.

Mr. RICHARD M. Haddock of Drexler Technology. He has been president since 1997 and of LaserCard, a Drexler subsidiary, since 1989. LaserCard makes optical memory cards and high security ID card systems. It is employed by the Immigration and Naturalization Service, the Department of Defense and the State Department. These smartcards are variously used as multiple entry visas for qualified Mexican citizens, as INS permanent resident cards, green cards, and as U.S. Army automated manifest cards. Last month LaserCard received a $4.8 million order for LaserCard ID cards for the current U.S. border ID card program. They currently make about 4 million cards annually for North America.

And then finally, Joanna Lau of Lau Technologies. She is the founder and CEO of Lau Technologies. This is a systems integration company with decades of experience in the development and delivery of high-end electronic systems for military applications and secure identification and surveillance systems. Lau Technologies and its subsidiaries provide security products to the Department of Defense, the FAA, the Department of State, and private industry.

I might say that the company created Viisage Technology, which develops facial recognition technologies. This company's products are used in a variety of ways, from screening crowds at last year's Superbowl to increasing security at airports, including Fresno International, to producing digital licenses.

So we will now begin with Miss Lyons and we will go right down the line. Welcome.

STATEMENT OF VALERIE J. LYONS, EXECUTIVE VICE PRESIDENT, WORLD SALES, IDENTIX, INC., LOS GATOS, CALIFORNIA

Ms. LYONS. Thank you very much. Good morning, Madam Chairwoman, Senator Kyl.

Identix is a biometrics company founded in 1982. We are the leading provider of fingerprint biometric technology for solutions with criminal justice, airport security and commercial markets, headquartered in Los Gatos, California with a significant presence here in the Washington metropolitan area. Our FBI-certified technology is currently in use worldwide to identify criminals, screen job applicants, control physical access, protect information and prevent identity theft and fraud in cyberspace.

Fingerprint biometrics are extremely accurate, easy to use and already deployed on a large scale. For example, all U.S. military recruits and current holders of California driver's licenses already have fingerprint images as identification on ID cards. As you pointed out though, no one is reading those cards. California teachers and day-care providers are fingerprinted for background checks.

With the implementation of the Airport Security Improvement Act of 2000, we are proud to have helped airports comply with mandated security improvements for the category X airports. Identix fingerprint biometric solutions are now in use for background checks at the majority of large airports. Those include Dulles, Reagan National, BWI, San Francisco, O'Hare, Logan, Orlando and Houston's Bush and Hobby Airports. Identix also provides applicant screening for United, Continental and Horizon Airlines. This law puts in place critical safeguards against potential threats and we urge Congress to expand its scope to apply to all airports.

At the back of this room—we can do demos later, as opposed to doing those right now—is an Identix fingerprint capture device. Those are used for criminal and job applicant screening at the airports that I just mentioned. In about 10 minutes time an operator can record a forensic quality fingerprint, 10 fingerprints, and then for job applicants this record is transmitted to the U.S. Office of Personnel Management, which forwards it to the FBI for a search. The results are sent quickly and confidentially to the prospective employers.

Now when these fingerprints are used as part of a comprehensive security effort, fingerprint applicant screening can prevent persons from being employed in sensitive jobs who have a criminal history, citizenship issues, or who might otherwise be connected with unlawful activity. It is important to remember that fingerprint checks are effective because there are databases against which checks can be made. Virtually all police and law enforcement networks worldwide and many border entry and visa control systems are fingerprint-based.

Fingerprint biometric applicant background checking is essential as the first step in authenticating employees in sensitive jobs. However, once their identity has been established, it is important to ensure that this identity is not compromised once they become employees and have access to secure areas and computers. Today employees are typically given a badge and the only connection between the badge and the employee is a picture on the badge. There

is currently no method of ensuring that the badge owner and the user is indeed the person that had the background check.

We can enhance security by putting the fingerprint image, which we captured during the applicant processing, on a badge, a smartcard, if you will, thereby creating that direct relationship between the individual, their badge and the background check.

This smartcard here has a chip on it and the image is on this card and no one can use this badge without me and my finger.

Chairperson FEINSTEIN. Could we take a look at that badge? Maybe someone could go down and bring it up; that would be very useful. Thank you very much. Please continue on.

Ms. LYONS. This is a biometric doorlock. So with the fingerprint image on that badge, you can also prevent or allow for physical access to secure areas using a badge with a biometric on it. It recognizes my finger image when prompted to do so by the badge and it will only open for me, with my badge and my finger.

The same is true for computers. Here is a reading device that can be used in concert with the badge to allow only access to my computer, again with my badge and my fingerprint, assuming my fingerprint image is on that smartcard.

So while my testimony is focussed on personnel security matters, this same approach can be applied to the frequent traveler to expedite check-in, boarding for the airline travel, and other forms of transportation. Like the employee ID, the frequent traveler card starts with a form of identity-proofing as might be prescribed by the federal government, something clearly more than a driver's license but several forms of identification to do identity-proofing. The finger image is placed on a smartcard so that the card cannot be exchanged or counterfeited.

However, unlike the employee ID, the frequent traveler card would keep the finger image on the card and not in a central database. This card would be voluntary. Its principal purpose is to authenticate the traveler, promote convenience and increase public confidence in our transportation infrastructure.

Fingerprint biometric solutions can raise the level of security for travelers without further raising concerns of privacy because they hold the image in reference to the traveler.

Madam Chairwoman, we appreciate having the opportunity to share our views with the Committee today. We commend you for your leadership in focussing attention on the role that technology can play in these challenging times. Your recently-introduced legislation promoting visa reform demonstrates another area in which biometric technology can be used to enhance homeland security. The use of fingerprint biometric technology is already widespread. The technology itself is reliable, cost-effective and proven.

The challenge we all face from 9/11 is to restore safety and traveler confidence. Any solution that Congress mandates or industry is asked to deliver must be deployed rapidly, reliably and integrate with existing processes and current investment. Fingerprint biometrics delivers on all those requirements. We would be privileged to do whatever we can to improve aviation and homeland security through the application of fingerprint biometric technology and we look forward to continuing to work with you.

[The prepared statement and attachments of Ms. Lyons follow:]

STATEMENT OF VALERIE J. LYONS, EXECUTIVE VICE PRESIDENT OF IDENTIX INCORPORATED, LOS GATOS, CALIFORNIA

Good Morning, Madam Chairwoman, Senator Kyl, and other members of the Subcommittee. My name is Valerie J. Lyons and I am Executive Vice President of Identix Incorporated. Founded in 1982, Identix is the leading global provider of fingerprint biometric solutions for the criminal justice, airport security and commercial business markets. We are headquartered in Los Gatos, California and have offices in Fairfax, Virginia and other cities in the U.S., Europe and Australia. Our technology is currently in use around the world. Our FBI-certified technology for capturing and managing fingerprint images electronically is used to identify criminals, screen job applicants, control physical access, protect proprietary information, and prevent identity theft and fraud in cyberspace.

Our fingerprint biometric solutions are extremely accurate, easy to use and already deployed on a large scale as a standard procedure. All U.S. military recruits and current holders of California drivers' licenses have had Identix finger images captured for purposes of identification. California teachers and day care providers are fingerprinted for background checks.

With the implementation of the Airport Security Improvement Act of 2000 in January, Identix fingerprint biometric solutions for background checks are now at the majority of large airports, including: Dulles, Reagan National, Baltimore-Washington, San Francisco, O'Hare, Logan, Orlando and Houston's Bush and Hobby airports. Identix also provides job applicant screening for United, Continental, and Horizon airlines. This law puts in place critical safeguards against potential threats. We urge Congress to expand its scope to apply to all airports.

On display is the Identix fingerprint capture device used for criminal and job applicant screening at the airports I just mentioned. In the law enforcement community this is known as a "livescan" or "tenprint" machine. Using this machine, the screening process is simple and straightforward. In about 10 minutes time, an operator can record forensic quality electronic images of the applicant's full ten fingerprints. For job applicants, this record is submitted electronically to the U.S. Office of Personnel Management, which in turn forwards the record to the FBI for a search of its Integrated Automated Fingerprint Identification System, known as the "IAFIS". The results of the IAFIS search are transmitted confidentially to the prospective employer within a window of time that varies from a few hours to no more than 72 hours. A search of this sort costs approximately $35 to $50 per applicant. The cost of the machine ranges from $20K to $40K depending on the functionality desired.

When used in a timely manner as part of a comprehensive security effort, fingerprint based job applicant screening can prevent persons from being employed in sensitive jobs who have a criminal history or are otherwise wanted in connection with unlawful activity. It is important to remember that fingerprint checks are effective because there are existing, "back-end" databases storing fingerprints against which checks can be made. Virtually all police and law enforcement networks worldwide and many border entry and visa control systems are fingerprint based. There is a worldwide network of skilled, professional fingerprint examiners and a core set of systems that are maintained and updated routinely, as a matter of standard practice.

Fingerprint biometric based job applicant background checking is an essential first step in authenticating employees in sensitive transportation and critical infrastructure related jobs. However, once this form of identity has been established for workers it is important to ensure that their identity is not compromised once they become employees and have access to secure areas and computers.

In many so-called secure enterprises today, employees are given an ID Badge for access purposes, however, this method does not ensure that the badge owner and user is in fact the person whose background was checked.

To test the integrity of any badging system we can ask 5 simple questions:

1) Is the employee who was cleared by the FBI the same person who receives the badge? The answer should be yes.
2) Is the rightful badge owner the same person gaining access through a door to a secure area? The answer should be yes.
3) Can the badge owner gain access through a door to a secure area without a badge? The answer should be no.
4) Is the rightful badge owner, the same person gaining access to a computer? The answer should be yes.
5) Can the badge owner gain access to a computer without a badge? The answer should be no.

We can enhance security through the concept of "continuity of authentication" for an individual's identity through the direct relationship between an individual, their badge, and the background check.

Allow me to demonstrate. On display is the fingerprint based job applicant system machine. Here is a smart card ID badge, with a fingerprint image on it. The background check results and my badge are tied together because they both have the image of my finger. No one else can use this badge without me.

This is a biometric door lock control. It can recognize my finger image when it is prompted to do so by this badge. It will only open for me with my badge and my finger. The same holds true for my computer. I insert this badge into a biometric enabled card reader that scans my finger and only I can enter a computer and exercise only the authorities assigned to me.

The "continuity of authentication" through biometric based badging offers greatly improved security that can be conveniently added to many existing systems for a relatively low cost. This approach can serve as a first line of defense against individuals who want to infiltrate airport facilities or other critical parts of the transportation infrastructure.

The U.S. Department of Defense paid $6 per card for smart card stock such as this. A computer can be locked down with biometric readers and software that are commercially available from most major brands of computer makers for about $100. Doors cost about $1000 per door in volume. Biometric based badging takes the next logical step to ensure that precautionary measures are in place in a way that maximizes background checks and physical access controls.

This technology and the concepts associated with it can be quickly implemented in transportation enterprises through timely and coordinated policy and management control. The General Services Administration has made smart ID badges available to the Executive and Legislative Branches through several vendors. Congress and the Administration should examine the merits of using biometric badging systems to improve the security of physical and computer access control systems in government buildings.

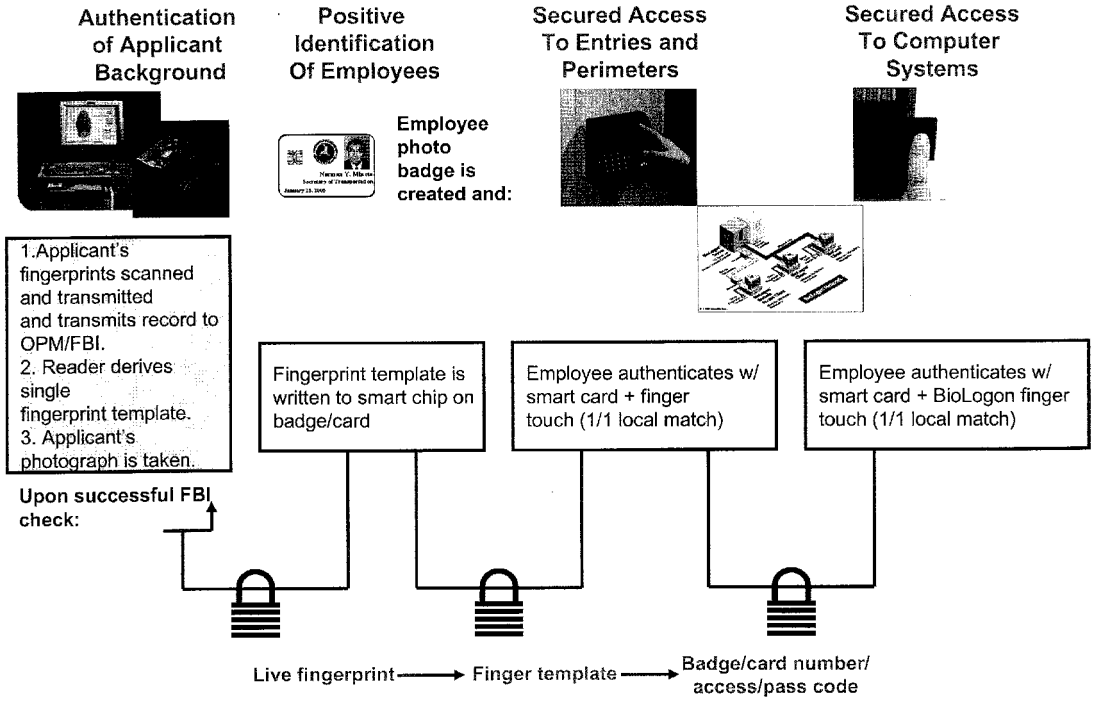
While my testimony has focused on personnel security matters, our approach can also be applied cheaply and conveniently to the frequent traveler to expedite check in and boarding for airline travel and other forms of transportation. Like the employee ID, the frequent traveler card starts with some form of identity proofing, not necessarily an FBI check, perhaps a bank process using applicable authority to check personal records. Also like the employee ID, a finger image is placed on a smart card so that the card cannot be swapped or counterfeited.

However, very much unlike the employee ID, the frequent traveler card would keep the finger image on the card and not in a central database. Also unlike a mandatory employee ID, a frequent traveler card would be voluntary, its principal purpose being to promote convenience and increased public confidence in the U.S. transportation infrastructure. There are very real privacy concerns with respect to the array of security solutions being considered. Identix believes that we can raise the level of security for travelers without undermining civil liberties.

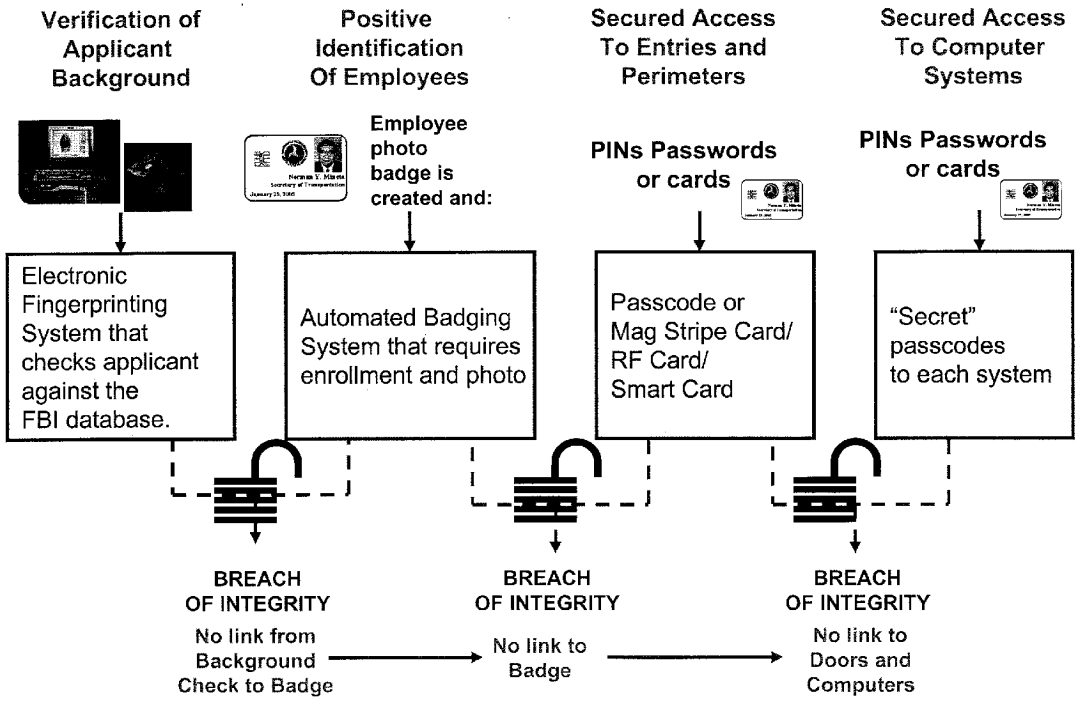
Madame Chairwoman, we appreciate having had the opportunity to share our views with you and your colleagues today. We commend you for your leadership and vision in focusing attention on the role that technology can play in these challenging times. Your recently introduced legislation promoting visa reform demonstrates another area in which biometric technology can be used to enhance homeland security. We would be privileged to do whatever we can to improve safety and security in our nation through the application of biometric technology. We look forward to continuing to work with you.

Thank you very much.

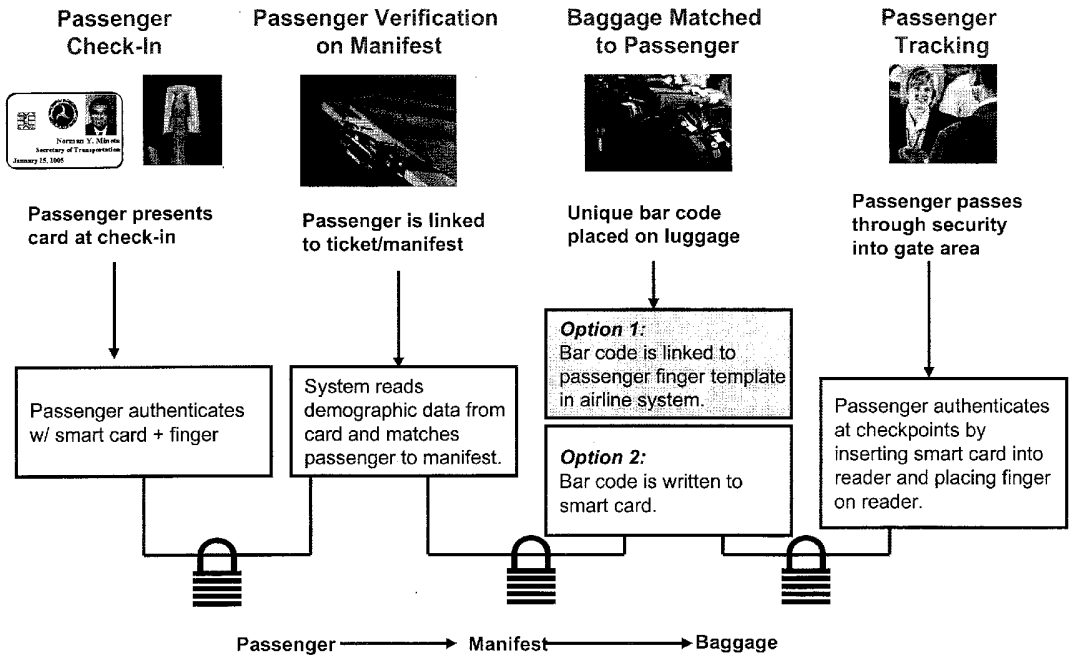
Continuity of Authentication for Airport Employees: Biometric Based ID Badges



Typical Environment:
Fragmented Employee Authentication



Frequent Airline Travel;
Continuity of Passenger Authentication Using Biometrics



SECURING OUR AIRPORTS AND AIR TRAVEL

PREPARED BY IDENTIX, INC.

IDENTIX AUTHENTICATES PEOPLE FOR SECURE AND TRUSTED ACCESS

AUTHENTICATING PASSENGERS AND PERSONNEL

SECURING PHYSICAL AND COMPUTER ACCESS

OVERVIEW

The seemingly impossible—four hijacked US airplanes and the ensuing tragedy—has proven all too real. In the aftermath, airport security has gone under the microscope for examination. And there is a common realization that restoring safety, security and trust to airline travel is critical to our National defense and public psyche.

However, it is important to realize that airport security concerns have been escalating for some time. Not only are airports "attractive targets" for terrorist activities, they also serve as magnets for criminal activities such as theft and smuggling. At the same time, airline and airport reliance on computer systems has opened the virtual door to hackers as another threat to our skyways.

Providing protection against these threats presents a special challenge. Because airports support activities that are both public—passengers, visitors and airport employees—and private—such as air cargo and mail—these locations are part transportation hub, shopping mall and industrial complex. As a consequence, requirements for public safety and security are a hybrid of both commercial and industrial needs similar to a small or medium-sized U.S. town or city.

The resulting challenge is to balance security, safety and government regulatory compliance with the privacy rights and convenience of individuals. Addressing this challenge is the lynchpin of Identix' airport security solution. Today, Identix is the leading provider of biometric security solutions for airports and other government-regulated organizations.

IDENTIX—AIRPORT SECURITY COMPONENTS

The Identix airport security approach components consist of products available today that can be integrated to:

Screen airport and airline workers before hiring to ensure no past criminal history;
Grant physical access rights to different airport locations easily;
Control access to computer systems; and,
Uniquely link passengers to their boarding pass, baggage and passport control.

FINGERPRINT BIOMETRICS

The approach is based on two Identix core technologies: fingerprint biometric software and hardware tied to the itrust access control platform.

Identix is the leading provider of finger biometrics for the criminal justice, airport security and enterprise markets. Its technology is used to identify criminals, screen job applicants, control physical access, protect proprietary information, and prevent identity theft and fraud. Several million fingerprint templates have been enrolled using its technology. Finger biometrics are accurate, easy to administer and convenient.

The itrust Internet access control platform supports multi-factor authentication, including finger biometrics, smart cards, facial recognition, etc. In addition, itrust is a complete authentication, authorization and transaction management solution that allows an airport to establish strict multifactor authentication policies to ensure the identity of the end-user while maintaining the confidentiality of the information.

IDENTIX OFFERS A FULL RANGE OF COMPONENTS TODAY

No other company offers physical, logical and passenger/personnel screening using the same method—the human finger—for immediate and cost effective implementation. Identix provides:

Positive identification and protection of privacy against ID theft;
Finger biometrics that are convenient, reliable and cost effective;

Criminal history identification database inquiries;
FBI-certified products;
Technology options and form factors to meet your needs; and,
Easy to use, comprehensive systems administration capabilities.

IDENTIX—LEADER IN PROVIDING BIOMETRIC PRODUCTS TO GOVERNMENT

Identix has been working with airports and government agencies regarding applicant screening for over 6 years. Already, the company has installed job applicant security solutions to the nation's largest airports including JFK International, Dulles International, Boston Logan, Chicago O'Hare International, Baltimore-Washington International, Reagan National, Orlando International and San Francisco International.

The Identix/Sylvan joint venture handles all job applicant screening for United, Continental and Horizon Airlines and a substantial portion of the American Transportation Association's screening needs.

Because of airport security concerns, Congress has mandated a high level of security vigilance and recent events promise even more legislation. For instance, the Airport Security Improvement Act of 2000 took effect in early 2001. This new law clearly signaled Congress' intent to improve passenger safety and airport security in the following areas:

Criminal history background checks for all airport employees coupled with identification badges for secure areas;
Restricted access to certain areas;
Baggage and cargo loading inspection; and,
Passenger screening to airport concourses.

Identix' airport security products not only address this recent mandate but also extends the security net to passenger authentication.

AIRPORT AND AIRLINE EMPLOYEE IDENTIFICATION AND ACCESS CONTROL

Airport security begins with the people who work there. It is critical that employees be citizens in good standing with no past criminal history. For optimum security, physical and network access should be controlled based on specific requirements of the job. The Identix approach addresses these issues and integrates identification with access control.

Personnel screening. Before an employee is hired—baggage handlers, airport vendors, ticket agents, etc.—background checks are performed using fingerprint images which are electronically submitted to the FBI's Integrated Automated Identification System (AFIS).

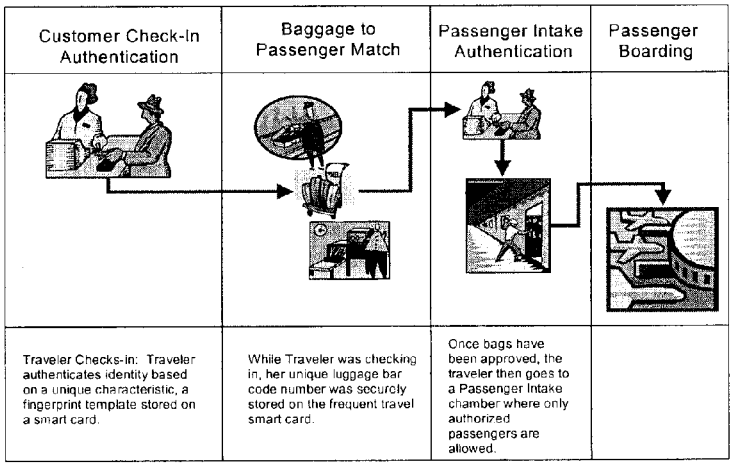
Employee ID issuance. Once an employee has passed the background check, demographic information can be matched with fingerprint templates stored in a centralized ID management server database and on a smart card.

Integrated physical and network access authorization. The centralized ID management server database defines each employee's authorization access path that includes both physical access and networks. Access to both physical locations and network nodes can be authorized for each location or PC and can require integrated access control. For instance, pilots may have access to the cockpit and all doors; reservation staff to internal terminal doors but not baggage areas and specified PC terminals; baggage handlers may be restricted to a few doors in certain areas, etc. A combination of multifactor authentication types may be applied depending on security requirements.

Roaming airline employee authorization. Pilots, flight attendants and other airline personnel routinely travel from airport to airport requiring authorized access to several locations. Identix provides a platform which can recognize and handles remote authentication and authorization.

SECURE PASSENGER TRAVEL SYSTEM

Day in the Life of a Secure E-Traveler



Passenger security requires knowing who the passenger is, where they go and what they have with them. This involves a continuous, exact match of travelers and their bags to an aircraft passenger manifest.

Frequent flyer ID card. As a service to frequent flyers who comprise almost 70% of air travelers, membership cards can include fingerprint templates that allow road warriors to move from one airport to another quickly. Because the smart card requires re-authentication—a touch of a finger—at each secured access point, security is not compromised and customer loyalty rewarded.

Check-in identification. When a passenger purchases a ticket at the counter or electronic ticketing kiosk, background checks are performed to identify known terrorists or criminals using automated fingerprint images that are electronically submitted to a database of known terrorists or criminals. Once a passenger has passed the background check, the fingerprint template is stored on a smart card or 2D bar code on the passenger's boarding pass.

Baggage control and matching. At the curb or at the ticket counter, each baggage claim ticket is marked with the passenger's same fingerprint template stored on a smart card or 2D bar code on the boarding pass. Now, airlines can easily and accurately match passengers on board with baggage in the hull. Upon arrival, matching the baggage claim ticket to the passenger can be accomplished in seconds.

Boarding identification. Knowing that passengers boarding a plane have been identified and cleared is crucial to security. At the gate, as the boarding pass is inserted into the kiosk, the passenger is authenticated once more using a smart card or 2D bar code on the boarding pass. This final step validates the passenger manifest and protects passengers from known criminals and terrorists.

IMMIGRATION, PASSPORT AND VISA ADMINISTRATION

Access to the U.S. from many countries usually requires a Visa. Imagine the value of identifying foreign visitors prior to a trip and linking identity to airline ticket and passport control. At the same time, native born and naturalized citizens can enjoy added security as they travel from country to country. Currently, some countries have already deployed Identix solutions for immigration control.

Visa and passport issuance. At time of issuance, travelers' background can be checked using automated fingerprint images and submitted to the FBI (or other agencies such as the INS) for a criminal and terrorist history check. The fingerprint template is stored on the Visa or passport as a 2D bar code or magnetic stripe or smart card.

Clearing customs. Upon country entry or exit, the passenger is re-authenticated with a touch of a finger and compared to the template stored on the Visa or passport. The process takes seconds and validates that the passenger is not a known terrorist or criminal.

IDENTIX BALANCES PRIVACY RIGHTS WITH SECURITY

Today, everyone understands the need for higher levels of security to protect the lives of travelers, visitors, and the airline and airport personnel who serve them. Yet the question remains, "At what cost to personal privacy?" Identix is committed to delivering biometric solutions that place a priority on maintaining individual privacy. At the same time, Identix provides the flexibility to engage and enhance security measures on an as-needed basis, so that security is appropriate to a person's particular role.

Identix believes in protecting an individual's privacy. Our minutiae-based algorithms analyze the position of the end points and junctions of print ridges and create fingerprint templates—mathematical representation of the print characteristics.

For identifying criminals or terrorists, the templates are used for identification purposes—the process of selecting one person's characteristics from a group of records. Called a "one-to-many" search, the question put to the system is, "Do you know this person?"The algorithm searches the database and returns a result of likely candidates. If no match is found, the template is deleted.

Verification, on the other hand, occurs when a person makes a claim to a specific identity. Called a "one-to-one" match, the question put to the system is, "Is this person who he claims to be?" The automated system compares the individuals measured characteristics against a previously registered record to determine whether the match is valid. The templates are used for matching purposes only and are destroyed at the match point.

Of course, the effectiveness of technology is determined by the people who implement it and create policies for its use. For this reason, Identix is committed to working with officials from airlines, airports and government agencies, as well as members of Congress and other policymakers, to implement biometric security practices that maximize safety while preserving privacy.

IDENTIX—ARCHITECTS OF AUTHENTICATION

Founded in 1982, Identix Incorporated (AMEX:IDX) develops, manufactures and markets the world's leading finger biometric software, hardware and services and an open Internet access control platform. Identix solutions are installed worldwide to protect proprietary information, prevent fraud and identity theft, identify criminals, control physical access, safeguard airports, screen job applicants and protect patient records. The leader in biometric technology, Identix believes it has enrolled millions of fingerprint templates worldwide.

Identix's products and services are categorized into three major groups:

Finger biometrics—Used in the enterprise to verify the person is who they say they are, Identix biometrics protect PCs, laptops, servers and PDAs from fraud and unauthorized access. Law enforcement and other government agencies use our biometrics to create forensic-quality images that can be transmitted directly to AFIS or other identification bureaus.

itrust—Internet access control platform leverages the efficiency of conducting business over the Internet while ensuring the trust and integrity of transactions with complete authentication, authorization and administration tools.

Consulting services—IT security, engineering sciences and complex project management services to the public and commercial sectors.

AIR TRAVEL SAFETY AND SECURITY RECOMMENDATIONS

1) *Expand the Airport Security Improvement Act of 2000 to All U.S. Airports*. The Act requires an FBI fingerprint background check for any individuals applying as a security screener, a screener supervisor, or one with privileged access to secure areas of an airport. The Act currently applies only to the 20 largest airports in the U.S. It should be expanded to include all airports in the U.S., regardless of size.

2) *Implement a Biometric System to Identify Those with Legitimate Access to Aircraft, Equipment, Computers and Secure Areas within an Airport*. Even before the September I I attacks, there were concerns raised about the level of physical and computer access security for-airport personnel. GAO investigators were able to carry weapons around two airport security checkpoints using phony credentials. Biometric technology, specifically fingerprint imaging, is currently being used to control personnel access at Chicago's O'Hare airport. Congress and the administration should

adopt legislation that would require the FAA to use fingerprint and other biometric devices to control physical and computer access at airport facilities. This effort could be accomplished through the use of a smart card ID badge issued to personnel containing a biometric identifier. With a fingerprint image biometric, based on an FBI background check, a lost or stolen card cannot be used by anyone else.

3) *Create an Electronic Watch List of Suspected Terrorist by Integrating Federal Agency "Back End" Databases*. One of the current passenger information shortcomings is the lack of coordination and communication among the various agencies monitoring, screening and finding suspected terrorists. So called "watch lists" are only as good as the "back end" databases and networks to which they are linked. Congress and the Administration should authorize the integration of these databases in order to create a more accurate and timely "watch list" of suspected terrorists and others involved in criminal activity. The INS, FBI, State Department, Interpol and relevant Intelligence agencies should be party to the database integration effort.

4) *Require a Biometric Enabled Match Among Passengers, Boarding Pass and Baggage*. One of the fundamental elements of airport security is information on who passengers are, where they go, and what they have with them. The recent attacks were a direct result of passengers on planes. In the wake of the TWA Flight 800 disaster, the govermnent commission analyzing findings called for a higher standard of passenger identification that ties the traveler to his or her baggage, boarding pass and flight manifest. This "iron triangle" of identity authentication provides: positive identification of all travelers at all points in the airport, including the gate; accountability for all checked baggage against boarding pass, and; complete and accurate passenger manifests. Congress and the Administration should adopt legislation that requires a standard for airline passenger identification derived from the principles of the "iron triangle" concept, thus enhancing airport and traveler security.

Chairperson FEINSTEIN. Thanks very much, Miss Lyons.

Mr. Willis?

STATEMENT OF WILLIAM WILLIS, CHIEF TECHNOLOGY OFFICER, IRIDIAN TECHNOLOGIES, INC., MOORESTOWN, NEW JERSEY

Mr. WILLIS. Good morning, Madam Chairman, Senator Kyl. I appreciate the opportunity.

I am representing Iridian Technologies. We are the developer of iris recognition technology, a superior biometric authenticator that can do both verification and identification. As part of our biometric, we do not require having a card. We can actually search a database very quickly in a matter of a couple of seconds and millions and millions of people. So you literally would not have to carry a second piece of identification. You just carry your eyes with you, if you will.

We are able to do that by taking a simple picture of the eye with a regular camera that is enhanced to be able to give a good quality component of the iris, which is the colored part of your eye. We are able to then do the authentication and make sure that it is totally distinct, as you said earlier, from any other person in the world.

Senator Kyl made a comment on how we could help specifically, if you will give me a moment. How can we use this for terrorist information? An example would be being able to put that at the borders of our other countries, be able at the visa point to take the picture of the iris, put that in a central database which only takes a few seconds, and I will be happy to show that to you, and then, at the time that they come back into the country, do the same test. You can then either do that with the card or without a card. That will be actually up to you in the deployment and in the cost scenario. If you choose to eliminate the cost of the card, you would not have to do that.

There are numerous third-party studies which are available upon your request that confirm that the iris is the most information-rich and accurate biometric. Iridian has developed these proprietary technologies to take advantage of the natural characteristics of the human iris to produce products both in physical and information security. Again I will show you in my five minutes both those things.

The technology is widely deployed today for both physical security in corporate America and in the United States government. New imaging products for major manufacturing partners of Iridian have created a situation where products are ready for deployment today on a very large scale.

Iris recognition is a natural identification component of anti-terrorist security systems. It is capable of high-speed, real-time, extremely accurate operations in a very large database environment, such as immigration and border security, national transportation system security, information network protection, and access control for security of critical infrastructure assets.

I have some examples of that. Schiphol Airport in Amsterdam, Netherlands is doing that for immigration control of the European Union, Heathrow Airport in London in the United Kingdom and Douglas International Airport again in Charlotte.

The tragedies of September 11 have made us keenly aware of the fragility of our nation's infrastructure. Iris recognition technology can rebalance the equation of open access and controlled access without sacrificing the rights of privacy and free movement in our society. Americans now understand that it is in the country's best interest to manage access to America's infrastructure by applying technology in a way that is efficient, reliable and trustworthy and Iridian Technologies standards ready to make its innovative products available to do that.

Chairperson FEINSTEIN. Thanks very much, Mr. Willis.

Mr. WILLIS. I have—

Chairperson FEINSTEIN. Would you like to show that?

Mr. WILLIS. I would like to show that in my five minutes. That is why I cut it short.

Chairperson FEINSTEIN. Proceed. You have your five minutes.

Mr. WILLIS. Hopefully I answered the question that you had, Senator.

Two quick ones. I will be able to log on. I have just looked at the camera. It has seen me, it knows that it is Bill and it is logging me onto the computer. This is what we see for information security. Obviously the physical security is only as good as the network infrastructure you are going to put on it so you make sure that the terrorism is not only at the physical layer but also at the information layer, as well. You can see that I can from a very comfortable distance be able to run this. I will be able to now use this. We see this as an example of being able to take access badge-readers off of places that are secure, be able to put the camera—you do not need the second factor, which would be a card—and be able to enroll.

As you can see, in a couple of seconds you have a picture of my eye and at the same time we have the ability to do an unlimited database search. So instead of a day or a few hours, you literally

could have the response within a few seconds if there is someone that would be suspected of looking into farther.

[The prepared statement of Mr. Willis follows:]

STATEMENT OF WILLIAM WILLIS, CHIEF TECHNOLOGY OFFICER, IRIDIAN TECHNOLOGY, INC.

Iridian Technologies, Inc. (Iridian) is the developer of iris recognition technology, a superior biometric authenticator that performs either verification or identification of a claimed identity. Identification is accomplished by a complete search of a database using a mathematical representation created from the image of the iris in the human eye. Images of the iris, the colored ring around the pupil, are acquired by a camera at a comfortable distance, and converted by algorithm into a secure IrisCode. This IrisCode is used as a template for comparison when a new eye is presented for authentication. Iris recognition technology is totally distinct from an earlier and unrelated approach, retinal scanning. Retinal scanning relies on an active laser probing inside the eye to view the retina at the back of the eye. Iris recognition uses the external colored part of the eye via a simple photographic image.

Numerous third party studies [available upon request] have confirmed that the iris is the most-information rich biometric. Iridian Technologies has developed proprietary technology to take advantage of the natural characteristics of the human iris to produce products that support both physical security and information security applications. Iris recognition was in development from the mid-80's, and its first products for physical security were deployed in 1996. The technology is widely deployed today for physical security in corporate America and the government. New imaging products from major manufacturing partners of Iridian Technologies have created a situation where the products are ready for deployment on a large scale.

Iris recognition is a natural identification component of anti-terrorist security systems. It is capable of high-speed, real-time, extremely accurate operations in very large data base environments such as Immigration and Border security, National Transportation system security, information network protection, and access control for security of critical infrastructure assets. Examples of scalable deployments include Schiphol Airport, Amsterdam Netherlands, Heathrow Airport, London United Kingdom, and Douglas International Airport, Charlotte North Carolina.

The tragedies of September 11 have made us all keenly aware of the fragility of our nation's infrastructures. Iris recognition technology can rebalance the equation of open access and controlled access without sacrificing the rights of privacy and free movement in our society. Americans now understand that it is in the country's interest to manage access to America's infrastructure by applying technology in a way that is efficient, reliable, and trustworthy. Iridian Technologies stands ready to make its innovative products available to achieve these ends.

Chairperson FEINSTEIN. Thank you very much. Very interesting. Thank you.

Dr. Atick?

STATEMENT OF JOSEPH J. ATICK, CHAIRMAN AND CEO, VISIONICS CORP., JERSEY CITY, NEW JERSEY

Mr. ATICK. Good morning everyone and thank you for inviting me to share with you my views regarding this timely subject.

I am the CEO and chairman of Visionics. Visionics is a company that has pioneered fingerprinting, as well as facial recognition. We supply livescan technology to all of the INS today, so all immigrants today that apply for citizenship have to touch the surface that we make to authenticate or to check that they do not have a criminal record. We are in about half of the category X airports in about 600 police departments and 300 courts.

That is not the part of the business that excites me because I see now a new generation of innovative technology in the area of fingerprinting that we are producing, which has to do with mobility. It has to do with the ability to deploy on-demand identification in the field. We have deployed in California for the first time ever in October a technology that allows officers in the field to capture

fingerprints, as well as facial images on a mobile device and to submit them to the local as well as the federal databases to establish if somebody is wanted for a crime. The first week of operation alone has produced 100 identifications of criminals, including six fugitives who were wanted for major drug warrants and outstanding warrants. So this is the power of identification and I think with innovative technology we can deliver it.

I want to focus on the other side of our business, which is the facial recognition part. This is a technology that I have been intimately involved with for the last 14 years when I used to be a scientist at Rockefeller and Princeton and it has to do with the ability of a computer to establish somebody's identity by looking at their image and measuring the physical structure of their face.

The way we are proposing to implement this technology in an airport environment would be to use standard video cameras that are attached to the frame of the security checkpoint. As people walk through that frame, the technology in real time and continuously, at a distance in motion, will capture every face, will scan every face, convert it into a mathematical code called your faceprint. Your faceprint is a very small amount of data, about 84 bytes of data, shorter than a quick e-mail message that you send to a friend, but it contains the physical measurements of your skull and your face and it is identity-specific. It is unique to you, it does not change with aging and it is not affected by viewing conditions and also not affected by superficial disguises. If you put facial hair, mustache, beard, change your hairstyle, that is not what the facial print is doing.

So what you can do is submit that faceprint automatically against a database of known terrorists and criminals so that you can ensure that every person boarding the plane has been checked against that database. If a match happens, an alarm sounds in an alarm-monitoring station, either at the airport or somewhere centrally, and then you can dispatch a message to the security at the checkpoint and say please interview this passenger because his facial structure matches a terrorist. It does not create new lines and it does not inconvenience the traveling public. It is just behind the scenes, matching faces against the watchlist.

Chairperson FEINSTEIN. Is it instantaneous?

Mr. ATICK. It is instantaneous. It does a million matches a second, so you cannot even measure the time it does it. But there are concerns and I would like to address them very quickly. This is, in my opinion, a powerful tool that should be added to the list of tools that we use at the airports, including the luggage scanning and the metal detectors, but there are two concerns that you have heard about and you will continue to hear about as you consider this technology. One is the concern for privacy and the other one is the concern for accuracy.

The concern for privacy has to do with the misconception that this is an ID system that is identifying every one of us. This is not a national ID system. It does not identify you or me. It is simply a criminal and terrorist alarm. If your face does not match one on the database, on the watchlist, there will be no alarm. There will be no record of you even going through the system. If there is a match, then somebody investigates. The key here is that Congress

should make sure that watchlists do not get expanded to include noncriminals.

On the issue of accuracy, I want to say that you may have been hearing a lot of conflicting statements, either from vendors or from people who have specific agendas. The fact is it is very hard to answer the question of how accurate is facial recognition in a responsible short sentence because it depends on the quality of the images and the degree of control that you can implement on the imaging environment.

Using databases that are available to the FBI and using that type of quality, which is all we have today, we have done extensive benchmarks since September 11 and we believe, as a responsible company, we believe we can deliver the probability of capture of a terrorist between 60 to 90 percent probability. I am not saying that this is the accuracy of facial recognition. I am saying given how bad the images are in the FBI databases, we can give you confidence that 60 to 90 percent of terrorists will be spotted as they go through metal detectors and checkpoints, with very low false alarm rate.

This, in my opinion, is a phenomenal performance because it means that it will deter terrorists from entering into these areas because there is a high probability if they do, they will be captured.

One final point. A lot of improvements are being done in this area. DARPA is funding a major initiative called Human ID at a Distance, which we are part of, and we are in the process of beginning to install at two U.S. airports next week, including a category X airport. We have been in Keflavik Airport for a couple of months now and the belief we have is that the experience we have gathered is going to allow us to form a consortium of airports that will be tied in together and submitting against a common database. We believe we will be able to work as an industry with the FBI and the FAA to establish standards, as well as potentially down the line a better understanding that would help them mandate this capability.

My final sentence is that as a scientist, I am proud to say that we have as a country a technology that can make the difference in the war against terror and we can make it responsibly and peacefully and I would like to see us as a nation embarking in evaluating this technology.

[The prepared statement of Mr. Atick follows:]

STATEMENT OF DR. JOSEPH J. ATICK, CHAIRMAN AND CEO, VISIONICS CORPORATION, JERSEY CITY, NEW JERSEY

Let me begin by stating what I see as the corner stone of our defense, as a civilized world against crime and terrorism in this new era:

"I believe it is our ability—in the context of a free society—to identify those who pose a threat to public safety and to prevent their actions."

Essential to the success of this defense strategy are two ingredients:

(1) Intelligence Data
(2) Identification Technology such as facial biometrics

Fact is, terrorists do not emerge overnight. They require indoctrination and constant reinforcement over an extended period of time. This affords intelligence agencies opportunities to establish identities of many of them and to build watch lists. Ultimately terror is not faceless.

Today, even without systematic cooperation between intelligence agencies there are watch lists that contain large numbers of terrorists and fugitives. Check out the FBI's website for the monthly posting's of fugitives.

According to published news reports—two of the terrorists in the September 11 hacking were already on a watch list and were sought by the FBI since August 23, a third was already known to the French authorities. I suspect we will find out several others were already known either to the Germans, Belgium, French, British or Israeli intelligence organizations.

While there is no guarantee that all terrorists will be known in advance—at the very least we have the responsibility to try to prevent the actions of the thousands already known.

Given a watch list, the question becomes: does the technology exist that can spot these individuals as they enter a country or attempt to board a plane?

The demands on such a technology are very high make no mistake about it. Such a technology has to be able to:

(a) Scale: in the sense that it should work across many security checkpoints at hundreds of airports and borders and not just one location.

(b) Sift through more than 600 million travelers per year in the US alone and spot terrorists and criminals among them without interfering with passenger flow or throughput.

(c) Function without infringing on the rights or inconveniencing the honest majority.

The good news here is that such a technology exists. It is computerized facial scanning such as the FaceIt® face recognition technology. I can speak about this technology because I am not only the CEO of Visionics, the company that has pioneered and commercially developed this technology but I am one of its main inventors. I have worked on facial recognition and identification technology over the last fourteen years starting with my days as a Head of Two research Laboratories in Academia.

The technology works as follows: FaceIt® automatically detects faces in the field of view of a standard video camera, in motion, at a distance and without subject participation. It converts each visible face into a mathematical code, which captures the relative measurements between the landmarks of the human face—know as the faceprint.

The faceprint is a code that only a computer could interpret. It is encrypted and cannot be used to reconstitute the image of the face. It is unique to a given face and it does not change with age, lighting or viewing conditions. It ignores facial hair or other superficial changes to the face. In a sense it is a fingerprint in your face.

The extracted live faceprint is automatically sent via the network to a watch list database-residing either locally at the airport or centrally say in Washington. If a match exceeds a certain confidence threshold, then a human operator at the control room confirms the match and alert local security guards to intercept and interview passenger. The whole process could be a few seconds. If there is no match then there is no memory—the image is dropped.

The system does not record, store or alter the watch list database in any way. The watch list database cannot be hacked into as it only accepts faceprint queries through the network.

Over the years, in the world of aviation security we have seen successive technology adoption to enhance security. Today at the security checkpoint, X-ray luggage scanners, metal detectors and chemical trace detectors are deployed to check for concealed weapons and explosives on our body or in our carry-on luggage. I see facial scanning and matching against a watch-list as an integral component in tomorrow's airport security systems.

It is time to ensure that airports are no longer safe havens for criminals and terrorists. The American public agrees. In a recent Harris Poll conducted after September 11, 86% endorsed the use of facial recognition to spot terrorists.

Still there are some questions regarding this solution that have come come.

I would like to quickly address two:

(1) On the issue of privacy: It is important to emphasize that the FaceIt® surveillance system is not a national ID, it does not identify you or me. It is simply an alarm system that alerts when a terrorist on a watch list passes through a metal detector at the airport. If there is no match, I repeat there is no memory.

Furthermore, such a system delivers security in a non-discriminatory fashion. FaceIt® technology performs matches on the face based on analytical measurements that are independent of race, ethnic origin or religion. It is free of the human prejudices of profiling.

We have gone further and have called for Congressional oversight and for Federal legislation to ensure that watchlists contain only individuals who threaten public safety and to penalize for misuse of such technology down the line. Congress will take action in due time but at the moment their priorities are focused on the real

and present danger of terrorism and not the theoretical potential for misuse down the line.

(2) Another question concerns the accuracy of facial recognition

How accurate is facial recognition?

There is no responsible short answer to this question as it depends on the quality of the images in the database and the degree of control. It also depends on whether you are performing 1-to-1 or 1-to-many matching and whether you can enroll people or must use existing images for watchlist. We believe facial recognition is as accurate as fingerprinting if you have control over all these variables. In the airport terrorist and criminal alarm scenario we do not have the luxury of enrolling terrorists, we have to use the information available to intelligence agencies.

We recently conducted scientific benchmarks on existing and simulated terrorist watchlists and they show that the probability of spotting any given terrorist can be in the 60–90% with low false alarm rates. This is phenomenal because it means that the majority of the terrorists and criminals will be spotted using current technology. This will deter terrorists from attempting to board planes because if they do there is a high probability they will be caught.

So we must think of facial recognition at airports as a tool like the metal detectors and luggage scanners are tools. They enhance security tremendously without being technologically perfect. A facial scanning system at the security checkpoint will alert security to investigate just like they do today when the metal detector beeps.

I would also like to point out that facial recognition is constantly evolving and advancing. The state of the art today is a quantum leap of where it was even a year ago let alone 5 years ago and of course with the accelerated R&D initiatives underway the technology will rapidly become even more reliable and robust. FaceIt® has already been used in real world environments and has produced significant benefits—Mexican Election System, police Mugshot systems in many places around the world, Criminal Alarm systems in London, Birmingham, England, Iceland International Airport, Tampa and so on and we are seeing accelerated real world adoption based on a real value proposition.

This week we have announced that we are beginning to install facial recognition technology at two US airports including one Category X airport. The two airports will remain unnamed until the installation is completed. These are in addition to what Logan is doing.

IN CONCLUSION:

We owe it to the traveling public to do everything in our capacity to ensure their safety. We have the technology today as a nation to peacefully and responsibly make a difference in the war against terror and to restore the publics trust in the travel process without a cost to the privacy of the honest majority. I see no legitimate objection why we should not do it.

Chairperson FEINSTEIN. Thanks very much, Dr. Atick.

Mr. Huddart?

STATEMENT OF MARTIN HUDDART, GENERAL MANAGER, RECOGNITION SYSTEMS, INC., INGERSOLL–RAND CO., CAMPBELL, CALIFORNIA

Mr. HUDDART. Thank you, Madam Chairwoman and Senator Kyl.

My name is Martin Huddart. I am the general manager of Recognition Systems. We were the first commercial biometric company in the world. We were found in 1986, based in Silicon Valley, California. We are now a division of Ingersoll–Rand, a Fortune 200, $9 billion company which has a significance presence in security and safety through a variety of products and services, including the Schlage Lock Company that is present in millions of households throughout the world.

Recognition Systems is certainly a tried and tested technology and my testimony today will hopefully demonstrate that. We have over 60,000 systems in 80 countries throughout the world and there are literally millions of people enrolled in our systems.

Hand geometry is the science of looking at the size and shape of your hand. We are looking at 31,000 datapoints making 90 unique measurements. The interesting part about this particular technology, it is very fast, as we will show in a demonstration later. It is also very reliable in a coupled of environments that I think relate directly to many of the environments we have talked about today, such as airports, which is a high volume application where you need to process large numbers of people, say at an immigration or airport access control points. And it is very robust for difficult environments—light, heat. We have outdoor units which operate at subzero temperatures.

As we have participated and listened to the on-going debate about using technology there is a continuum that starts at experimentation and goes through implementation. It is our view we are very much on the implementation end of the spectrum. The reason is that this technology, many technologies are available today and have already been implemented by many private sector companies but also many government agencies, and that is what I would like to focus on. I want to talk about what has already been done, as I think that is a way to look at what can be done further, in two key areas that were mentioned in earlier testimony. One is immigration, identity verification, which could also include passenger verification, and then also access control to critical facilities in our national infrastructure, including airports as a key example.

So let us start out with immigration identity verification. One of the tasks here is we have a very large haystack to look through. Our technology is already being used in programs which prescreen travelers through immigration points, which allow the immigration officials to focus on the higher-risk passengers, and that is leveraging our resources more effectively.

Inspass is a system that is already using biometrics for immigration in the United States and Canada today and it has been doing so for the past seven years. Over 50,000 frequent travelers to the U.S. are enrolled in this program where they can bypass often the long immigration lines at nine North American airports, including Dulles, San Francisco, JFJ, Newark. Passengers approach this kiosk that you can see on the screen. They use a card, the card is used to claim who they are, and then the biometric, in this case hand geometry, is used to verify that they are actually who they claim to be, and this allows expedited arrivals back into the United States.

A similar system is in place today at Ben Gurion Airport in Tel Aviv, Israel, one of the world's most security-conscious airports. Twenty-one kiosks process 50,000 passengers per month today. This is not a trial; it is in process today. The line to get through immigration can go from 60 minutes down to 20 seconds by verifying the identity of those frequent travelers back to Israel. This system will be shortly expanded to the Israel–Palestinian border where both hand geometry and face recognition with Visionics is being used at the land border, also.

The second area that biometric technology can be used in the war against terrorism is employee identity verification. We have talked a lot about the fact that cards are not people and biometrics

is a way to go beyond the security that simple card technologies give us today.

The nuclear industry were the first industry to widely adopt biometrics. Over 90 percent of the nation's nuclear facilities use hand geometry readers and recognition systems to validate the identity of the employees going through the facilities and it has been installed for over a decade at many facilities, supported by the Department of Energy.

Airports. We have talked about San Francisco airport is the only fully deployed biometric system in the country where all airport operations doors are protected with biometrics, with over 30,000 employees using the system today. It has been in place since 1991.

FAA regulations currently specify that only authorized people are allowed access to the operations areas and San Francisco has been very aggressive in interpreting that to mean badges are not people; people are people, and using biometrics validates that. This was installed during your tenure as mayor of San Francisco, Senator, and you are welcome to come visit and you may have seen the readers at San Francisco as you have passed through there many times.

Seaports is another area of risk for national infrastructure. Rotterdam, the world's largest port and the gateway to European commerce, uses hand recognition technology to identify and validate the truck drivers who come into the petrochemical storage areas, a key area that you want to make sure only authorized people are allowed access to.

Many, many government facilities have already adopted this technology, including the Pentagon, the State Department, DARPA, several post offices, Federal Reserve Bank, which you see in the picture. Many American embassies, which have also talked about today, use this technology to protect their facilities, and many state prisons systems do the same.

Private industry has been a long adopter also of this technology. For example, the NASDAQ uses this technology to protect their service from unauthorized access, to protect the trading. Many research labs, banks, office buildings, colleges, schools, even day care centers use this technology to make sure only authorized parents pick up the children.

So I will leave you with the words, this is not a test. Usually in a security environment that is not a good statement but this is actually good news in that we have a significant library of identity verification solutions already in place and those solutions can be copied and pasted to many different areas of risk within our nation.

And if I can do a very quick demonstration that lasts 30 seconds?

Chairperson FEINSTEIN. Fine.

Mr. HUDDART. If I can ask Gordon to help me here, I will come around so you can see. This is an example of the smartcard, which I enrolled Gordon earlier with. It is a contactless smartcard that is a biometric template. You can see by the green light at the top of the unit that his identity was verified. If I get possession of Gordon's smartcard and I try to use it for unauthorized access, if you watch the top of the panel you will see the red light and I was rejected and we keep a record of that event having taken place.

I would like to present you with your own card.

[The prepared statement of Mr. Huddart follows:]

STATEMENT OF MARTIN HUDDART, GENERAL MANAGER, RECOGNITION SYSTEMS, INC., CAMPBELL, CALIFORNIA

Madam Chairwoman and members of the Senate Subcommittee on Technology, Terrorism and Government Information:

Good morning. I am Martin Huddart, General Manager of Recognition Systems, Inc. (RSI) based in Campbell, California, in the heart of Silicon Valley.

We are a pioneer in the application of biometric systems. Our primary technology is Hand Geometry. RSI's HandReaders have been installed in high security environments around the United States and worldwide since 1985. Today, there are more than 60,000 HandReader systems installed in 80 countries around the world, reading millions of hands every day. We are the industry leader in providing biometric technology solutions that protect important U.S. economic, energy, military, and transportation infrastructure.

RSI is a division of Ingersoll-Rand Company (IR), a Fortune 200 diversified industrial manufacturer and a world leader in security and safety. RSI and IR provide integrated security solutions—including hardware, biometrics and electronic technologies, software applications, maintenance and consulting services to government, military, commercial and industrial customers.

RSI's technology solutions have been installed in high-security, high volume access control environments for more than a decade. These include over 90 percent of the nation's nuclear power plants, as well as in leading scientific laboratories, Federal prisons, commercial airports, U.S. military bases, seaport cargo facilities, hospitals, universities, government buildings, industrial plants and commercial office buildings. Our technology is even used at day care centers to protect unauthorized persons from having access to the children.

In the wake of the terrorist attacks on September 11, one task is certain: we must significantly increase and upgrade security not only at U.S. commercial airports, but at other critical national infrastructure that could potentially be targeted by terrorists. The President's establishment of the Office of Homeland Security is an important initiative to better coordinate the efforts of more than 40 Federal agencies. Hearings like this—and others that RSI has participated in the past month—can help legislators better understand existing and new technologies, enabling you to make critical policy decisions that will better protect America's important infrastructure from future terrorist attacks.

Biometric systems lie at the core of technologies that can provide heightened security at a variety of infrastructure installations. Biometrics is the science of using physical characteristics to identify an individual. Modern biometric systems were developed in the 1970s. Early commercial products were expensive and therefore limited to very high security applications, such as nuclear facilities and laboratories. In recent years, developments in microprocessors and advanced imaging electronics have greatly reduced the cost and increased the accuracy of biometric devices. These developments have made biometrics increasingly common in commercial applications for access control, and even accurate personnel time and attendance monitoring.

RSI's HandReader was designed to be used in high-volume environments, where the identity of hundreds or even thousands of individuals must be accurately verified in a quick and efficient manner. These devices ensure that only authorized individuals gain access to specific places. This technology has been engineered to work reliably for a wide variety of users in difficult operating environments, including even sub-zero outdoor applications. The accuracy, reliability, durability and successful track record of biometric hand reading technology is unparalleled in the industry.

Members of Congress and Federal and local authorities have been inundated with proposals for new technologies since September 11. This includes many different biometric systems, including hand, iris, fingerprint, facial and voice recognition. While there is no disagreement that technology has a vital role in finding new security solutions for U.S. infrastructure, we must understand that this is not the time to experiment with new and unproven systems. Only those technologies and products that have already been proven in high-security environments, and which have an established reputation for performance, should be in the forefront of our decision-making processes in the weeks and months ahead.

To this end, one fact is well-established and should be clear: Of all the biometric systems currently in use, hand readers are the technology that today best meets the essential tests of performance and reliability in high-security environments. This is

a mature system that can be put in place quickly to meet a variety of security applications. That is what differentiates this technology from others.

This technology can be used for different types of security applications. One is preventing unauthorized employees from gaining access to specific areas and assets. Another is to quickly and efficiently identify low-risk users, such as pre-screened airport passengers, so that security personnel can focus on a much smaller category of people—high-risk passengers. RSI HandReaders can reduce the size of the haystack, so we have better chance of finding the needle in it.

RSI has worked with several U.S. Government agencies over many years to incorporate biometric systems into their security infrastructure. We have worked with the Immigration and Naturalization Service, U.S. Department of Energy, General Services Administration, Federal Bureau of Prisons, Drug Enforcement Agency, The Federal Reserve Board, U.S. Department of State, Federal Bureau of Investigation and most branches of the U.S. armed forces.

The Department of Energy has long realized the weaknesses of conventional card based access control systems at nuclear facilities. Concerned with stolen or forged access cards, 90% of the nation's nuclear facilities installed HandReaders at sensitive access points during the 1990s. These installations are not new, they are not a test, and they work reliably.

Given the new security concerns created by the terrorist attacks of September 11, I would propose that this proven model of security needs to be applied to other critical elements of our national infrastructure such as airports, power plants, chemical plants, port facilities, and transportation control facilities. There is a critical role for Congress and Federal regulatory agencies to play in mandating that new security procedures and technologies be put in place.

Nowhere is there a more immediate security challenge to address than that of U.S. commercial airports. Already, this Congress and the Department of Transportation have proposed several new initiatives. Some of these will take time to implement. One example of how we can very quickly improve airport security would be for Congress to improve existing Federal regulations to reflect the new security environment we all face. For example, the Federal Aviation Administration's directive FAR 107.14a mandates that only authorized people are allowed access to flight operations at commercial airports. Most airport authorities used card-based access systems to implement this mandate. These systems are inadequate because they can only accurately identify cards, not people. Only a biometric system that reads an individual's hand to provide positive identification of that person can do this.

One U.S. airport which has correctly interpreted the intent of this FAA mandate is San Francisco International Airport (SFO). At SFO, all 30,000 airport employees use RSI HandReaders throughout the entire facility. This is not a pilot program or a demonstration project; it is an integral component of the airport's security infrastructure. It has been in place for more than a decade. This system was installed during the Chairwoman's tenure as Mayor of San Francisco. I would urge other members of the Subcommittee and the Congress to examine how this technology has been used at SFO and to consider utilizing it throughout our national air transportation system.

In addition, while we applaud the Federal government's interest in exploring new security technologies through "pilot" projects, we must understand that these will take time to identify, test and implement. Time is our enemy. Therefore, we can ill afford to delay bringing the added security benefits of proven biometric applications while we investigate potential future enhancements.

At the top of any national priority list must be the desire to improve security and procedures at U.S. airports, seaports, land border crossings and high-profile government buildings. In each of these areas, hand geometry biometrics is already in use in some of the world's most sensitive security environments:

> RSI HandReaders are used not only at San Francisco International Airport and several other leading U.S. airports, but also at Ben Gurion International Airport in Tel Aviv. Passengers returning to Israel insert a simple credit card into a biometric kiosk as a means of presenting their identity. This identity is verified through the placement of their hand in the kiosk. Successful processing can be achieved in 15 seconds, much faster than the hour it can take to clear the regular immigration lines. Similar biometric immigration kiosks have been in place for the past 7 years at 9 North American airports including Dulles, JFK, Newark and Dallas airports as part of the INS sponsored INSPASS program. With over 50,000 frequent travelers enrolled in the program, there are 23,000 pre-screened passengers per month using this immigration process.
>
> A voluntary frequent traveler program is very powerful because it allows officials to focus resources on higher risk individuals and allows pre-

screened passenger travelers to proceed quickly through airport security. I will demonstrate how a proximity smart card loaded with a biometric template can be used to validate a passenger's identity in such a program. Also, our vision is that biometric screening processes can be applied to the check in and security check points of an airport, to make sure that the person who checked in is the same one who entered the plane.

In addition to the airport, the Israeli border crossing application will be extended in 2002 to the provide security at one of the most high-profile land border crossings in the world—the Israeli-Palestinian border crossed by more than 50,000 individuals daily. Again, biometric solutions will help manage visa and immigration procedures by reducing the risk of identity fraud.

Our technology solutions are used at the port facility in Rotterdam, Netherlands, the world's largest seaport facility and the primary sea transport gateway to the European continent to verify the identity of truck drivers accessing petrochemical storage areas.

U.S. Federal agencies use RSI's HandReaders at sensitive government installations including the Pentagon, U.S. military bases, the State Department, the NSA, DARPA, the US Postal Service the Federal Reserve Bank and American embassies abroad.

HandReaders protect access to hundreds of critical computer server facilities including the computers which run the Nasdaq stock exchange.

During the 1996 Olympic games in Atlanta, HandReaders reliably secured access to the Olympic village so that only athletes and authorized personnel entered the secured area.

As our nation moves forward following the tragic events of September 11, the overriding security issue will be to better manage identity verification and access control in a variety of high-volume environments. While machines can never fully replace highly trained and vigilant officials, a biometric hand reader will not get tired at the end of the shift, it will never take a day off, it won't "loan" its access code to cousins, friends or co-workers, and it won't accept a forged identity card. When integrated with other security technologies and procedures, hand geometry readers can significantly cut down the risk of unauthorized individuals gaining access to places and assets where they can cause damage.

I'd like to leave this Subcommittee with a piece of good news. The good news is that we can copy from a large library of proven identity verification solutions, then cost effectively paste these into the highest risk applications of our choice. We urge this Subcommittee, the Congress and Federal agencies to support the adoption of processes and technologies which will validate the identity of those accessing our borders, airports, ports and other critical national assets.

Thank you.

Chairperson FEINSTEIN. Thank you. Thank you very much, Mr. Huddart.

Mr. Haddock?

STATEMENT OF RICHARD M. HADDOCK, PRESIDENT, DREXLER TECHNOLOGY CORP., MOUNTAIN VIEW, CA

Mr. HADDOCK. Thank you very much. I thank Senators Feinstein and Kyl for having me here today. I only discovered yesterday at noon that I was able to come so my remarks are perhaps briefer.

One thing I would like to point out is that Drexler Technology Corporation has been the manufacturer of optimal memory cards in Silicon Valley for over 10 years and has been the supplier to the INS for both the INS's green card, permanent resident card, as well as the Department of State's border crosser card since 1997 and the supplier to the U.S. Army since about 1991.

The main feature of optimal memory cards is it how very large capacity. It has about 500 times more capacity than any other type of data storage card used in a wild-type environment and coupled with that, it is a very secure medium that allows data to be written to an area of the card only once, meaning that if you put a biometric on, say, track 1,000, you know that no one else can ever change

that. This is a key feature that caused the INS to adopt the card, to upgrade from their previous pink paper card, and essentially stopped all the counterfeiting and fraud that they had from that purpose.

But these cards contain biometrics. They contain the digitized color photograph of the card carrier. They contain what the INS views as an FBI-quality high resolution greyscale fingerprint. From that fingerprint can be extracted minutia from any formats because there are a number of proprietary minutia formats in the industry and the INS wanted to have a format that crossed industry boundaries and therefore, they wanted a high resolution image that could be used anywhere by anyone if they so authorized it. So it is a flexible biometric in that form. They have a digitized signature.

And in the Department of State version, which was implemented a year later, they also have two different fingerprint minutia templates.

To date there are about 10 million of these two cards in circulation in the United States held by permanent residents and Mexican citizens entering the United States and as such, it represents the highest security card in the country, the only card containing that type of biometrics in the United States and certainly one of the most secure cards in the world in our opinion, as well as at INS Forensics Department.

Part of the thing that I would like to testify here today at your panel is that we have been making these cards for over 10 years and there has been a great deal of interest in putting biometrics on the cards because of the high data capacity. I am probably the only one here that has business dealings with everyone on this panel. I have teamed on subcontracts with some; I have been resellers to others. Almost all of these technologies have been implemented successfully with optical memory cards so for more of an end-user point of view, we have a look at all of the biometrics that you are discussing here today. And having been involved in looking at biometrics for the past 10 years, we feel that we agree with your view of the fragmentation of the industry. All of these biometric devices have strengths and weaknesses and we have come to the opinion that the best thing that can be done is to put more than one biometric on a card. I do not think you can choose the right one. I think that it takes more than one and the type of biometric that should be applied is application-specific. I think the FBI testimony pointed that out earlier.

I think starting off with an FBI-cleared personal clearance so you know that you have the right person I think is the right basis of issuing a card but after that you can add any types of biometrics you want. Essentially with the data capacity available in our cards you can put everybody's biometrics on this card today. You can verify face, hand, fingerprint, any type of biometrics, and use them randomly and selectively.

This is a key factor because if you choose only one biometric, people will focus on that and there can be ways to break any given biometric if that becomes the standard for the country. So we feel it is much better to include multiple biometrics and be able to choose them as you need them and randomly, perhaps. Sometimes you use a fingerprint; sometimes a hand.

Additionally, you want to be able to upgrade this. The cards you issue need to be available for a long period of time. The technology will change; the templates will change. You want to be able to add that new technology to the card or adapt it without having to reissue cards. And having a secure medium to build on, you have the ability to do that.

In my testimony there are a number of references to programs that we have done with many of these vendors and we found the advantage of multiple biometrics in actual practice. So what we would like to recommend, one thought to leave you with is whatever the solution is, that you should consider multiple biometrics and also allowing those biometrics to be used selectively and perhaps even randomly, given different types of security concerns at different points of entry, and so forth.

So that is the substance of what I would like to say today and I am available for any questions you may have.

[The prepared statement of Mr. Haddock follows:]

STATEMENT OF RICHARD HADDOCK, PRESIDENT, DREXLER TECHNOLOGY CORPORATION, MOUNTAIN VIEW, CALIFORNIA

Madam Chairperson, distinguished members of the Senate Subcommittee on Technology, Terrorism, and Government Information, my fellow panelists:

Thank you for the opportunity to share my professional opinion with you regarding the application of biometric identifiers in our global war on terrorism. My name is Richard Haddock. I am President and Chief Operating Officer of Drexler Technology Corporation, a public company located in Mountain View, California, and traded on the NASDAQ as DRXR. We market our optical memory card products through our subsidiary, LaserCard Systems Corporation.

I have personally been involved with the invention and commercialization of highly secure optical memory cards for more than 20 years. These unique cards—called LASERCARDS®—have come to be known as the "world's most counterfeit resistant" identification cards.

This technology was invented here in the United States by Drexler Technology, an American company. Drexler manufactures optical cards and systems for sale worldwide from our facilities in Silicon Valley. I am here today because my company has extensive experience utilizing various biometric technologies as part of the unique security design of an optical card identification system.

Each of the technologies discussed by my fellow panel members could be and, in some cases, already are being used in secure optical memory card identification systems. In fact, ALL of the technologies described here today, plus others currently available, could be combined on one card to facilitate various levels of secure authorization and multiple site interfaces without the need for a central database of personal information or required on-line access everywhere identification is needed.

I would like to organize my remarks into three parts—

1. How to best use biometric identifiers for personal identification;
2. What a secure identification card is;
3. Field experience with biometrics on secure ID cards

HOW TO BEST USE BIOMETRIC IDENTIFIERS FOR PERSONAL IDENTIFICATION.

It is important at this point to recognize that I am a technologist and not someone who makes public policy. However, as an American, I can also see both sides of the long-standing debate over personal privacy as it relates to recent discussions in the press about national databases and even a national ID card.

I enjoy my personal freedoms but I am also greatly disturbed by the ease with which innocent people can be horribly impacted by persons having criminal intent—whether it be by gaining unauthorized access to our Nation and its services or by simply stealing one person's identity.

This must stop. And, we have the technology to do so today.

From my perspective in the Silicon Valley, it seems that the primary focus of the current national identification debate is (1) whether or not we need a national database containing each citizen's personal information; and (2) whether the American

public would feel comfortable having to show an identification card to receive services.

From my perspective, there is no question that there needs to be some form of national database or, at the very least, a sharing of information between key databases to ensure that threats are identified and cannot hide. Without such information, how could we ever expect to issue valid personal identification of any type?

The issuance of personal identification, such as drivers licenses, must be based upon an assurance that the persons being provided such documents are who they say they are and, further, that they are qualified to receive specific services and are not perceived to be a threat to those services or for any other services for which the personal identification might be used. The only way to do this is to check their applications against databases deemed appropriate by the issuing authority and positively identify them each time they request controlled services, such as air transportation. However, those databases do not need and should not contain personal information about our citizens.

The requirement that I show personal identification to receive services has never concerned me, nor does it appear to concern the majority of Americans.

In addition, I must have shown my drivers license at least a dozen times just getting here to meet with you today. It seems that everyone wants to see a "photo ID" these days. Unfortunately, I would be very surprised if anyone who inspected my drivers license could really tell if it was a valid ID and that I am really who I say I am.

That's where biometric identifiers come in.

As you might expect, my primary concern is the security of the personal identification document, itself—how certain can we be that the document is valid and that the person presenting it is in fact the person authorized by it? This is true whether the document is a passport, visa, pilot's license, drivers license, or frequent flyer card.

We can no longer permit any identification document, like a drivers license, to be used for higher level authorizations, like airline passenger check-in, without first considering the security level of the issuance criteria and the security of the document, itself.

It is this fundamental fact that tends to lead us all into the debate about central databases and national identification. In my opinion, such a debate is not necessary.

One central identification database or on-line identification card will not solve our Nation's security problem—it is far too complex an issue. Such a solution would merely create more problems by requiring that extraordinary amounts of personal information must be kept in central databases for even the most basic level of service request.

Even beyond privacy concerns is the technical reality that highly centralized, on-line systems are subject to overload, system-related failures, hacking, and cyber-terrorism. Creating a central database, national identification system that is always online could provide a single point of failure for our entire society if our enemies ever targeted it.

WHAT A SECURE IDENTIFICATION CARD IS.

No matter whether it is a drivers license or frequent flyer card, a secure identification card is a personal identification document, which verifies that a person is who he says he is, is not a threat, and has authorization for the requested service or activity.

As I have said, authorization for the requested service or activity must be determined at application and re-validated periodically during the life of that authorization. This requires some form of national database screening at a level consistent with the security needs of the authorization. Such checking can also be used to verify that the person is not a potential threat.

Verifying that the person is really who he says he is requires three things: (1) a secure identification card that cannot be easily counterfeited; (2) a biometric means to link the person to that card with certainty; and (3) a secure automated interface to verify that the person and card links are valid.

To avoid privacy concerns, the databases used during application should only be those determined to be relevant to the requested services. All other personal data, including biometric identifiers, should be retained by the individual on his or her secure identification card.

How would this work?

When an individual requests specific services or benefits (for example, an airline frequent flyer card to minimize check-in delays), an application would be submitted, reviewed, and approved. Next, a secure card would be issued containing multiple bi-

ometric identifiers, which can be read and verified by automatic readers at access or authorization points.

When the cardholder requests specific services (such as e-ticket check-in at an airport kiosk), the cardholder's identity can be quickly run against an on-line threat database without any personal information being transmitted from the card. Moving through screening stations, such as carry-on inspection and gate check-in at an airport, can be accomplished with off-line access control readers. The cardholder would be matched against a selected biometric or combination of biometrics found on his or her card (such as a fingerprint, iris scan, face, hand, or finger geometry). The time required to make such a match, linking the cardholder to the card, is less than 5 seconds.

Please note that I suggested a "*selected biometric or combination of biometrics*" in this brief scenario.

Biometric identifiers are not perfect. Each has a margin for error. To avoid rejection as well as the possibility that someone might try to defeat a one-biometric system, multiple biometric identifiers are highly recommended.

We have also found that not all locations will necessarily want to use the same method of biometric identification. In fact, our experience indicates that there is considerable interest in using a random combination of biometrics so that the cardholder will not know what biometric is being evaluated at any given time. This is definitely possible with current technology.

Field Experiences with Biometrics and Secure ID Cards

The product we manufacture, the LASERCARD® optical memory card, has the highest memory capacity of any standard ISO credit card format. This capacity is about 200—500 times more than the highest smart "IC" cards on the market today.

More importantly, we have had this high capacity card in the market for more than a decade, which has allowed our users to implement any and all biometric solutions offered in the market for many years, including all you have heard about here today.

It is due to the optical card's ability to store multiple biometric files and templates that almost all industry biometric devices have been linked into optical cards, and in most cases, more than one type of biometric data has been stored. The permanent, non-erasable laser recorded media makes optical cards the natural vehicle for secure, biometric based ID cards.

Examples of these applications include, most significantly, the US Immigration and Naturalization Service's Permanent Resident Card (the "Green Card"), which contains about 80,000 bytes of biometric information. Biometric files are stored in an INS secure partition on the card, accessible only through the use of INS controlled secure field readers. Included in this data zone are:

High quality color image of the card holder (as printed on the card surface);
FBI quality gray scale fingerprint image of the card holder; and
Digitized image of the card holders signature

Additionally, the US Department of States' "LaserVisa" border crossing card for Mexican citizens entering the U.S. has the same technology used on it, but adds even more biometric information to the card by the addition of two fingerprint minutiae files on the card to supplement the full image files stored.

Together, with more than 10 million of such cards in circulation within the US today, these cards represent the largest high security, biometrics-based, ID card program in US history. It is estimated that by the end of next year, this total will rise to 20 million cardholders.

Many smaller programs have been launched using optical cards and biometrics in the past 10 years, and these programs give a good insight into what is necessary to achieve a secure and cost-effective ID card system.

We have teamed with Unisys to design a border entry system using both Iris Scan and Digital Persona fingerprint systems.

We have worked in Hong Kong on the implementation of a pilot immigration control system there using both Identix fingerprint scanners and Recognition Systems Hand Geometry Systems.

We have implemented Identix fingerprint scanners for a banking card in the Czech Republic, and have supplied hand geometry systems to our resellers worldwide.

We have implemented signature verification systems using Checkmate systems, and those from CIC. Our cards have been used with voice recognition and face recognition, as well as two finger "Digi-Two" finger geometry biometric systems.

In short, we believe that we have the most extensive biometric based experience of any card supplier, since we have always had the ability to store and implement

any and all biometrics from a single card. No database connection is required for our totally off-line verification system approach to these biometric systems.

Based on this long-term experience with all forms of biometric devices, we have developed our own view of the best approach to a biometric ID system. The key elements of such a system are:

Implement more than one type of biometric;
Allow room to add new biometrics seamlessly;
Assure off-line verification ability;
Provide for selection of appropriate biometric based on application requirements; and
Assure integrity of the biometric files from issuer to user.

Explaining in more detail:

IMPLEMENT MORE THAN ONE TYPE OF BIOMETRIC:

There is no perfect biometric system. All systems have their strengths, weaknesses, and vulnerabilities. The selection of a single biometric for any large-scale system invites a concerted effort to defeat any given biometric, which will be done. This was the experience in the Hong Kong pilot, where both fingerprint and hand geometry systems were targeted by the test system, and both were shown to have vulnerabilities. The same is true for Iris scan and face recognition systems. Examples of failure modes include false fingertips, rubber hand molds, glass eyes, contact lens, and actors face make-up techniques.

Adding to the complexity is the need to accommodate the disabled and handicapped in any public access system. Considerations include:

IrisScan system needs to accommodate the height ranges from children, wheelchairs, and basketball players, blind eye without eyes or glass eyes.
Hand Geometry system needs to work in hand size ranges from small children and Asian women's hands through football players, plus the fact that not all people have right hands. Sanitation concerns must be addressed as well, given concern over germs and disease.
Fingerprint systems need to address the same sanitation concerns as Hand Geometry, plus the ease of false fingertips and other substitution methods. Proprietary template algorithms and changing standards need to be addressed as well. The fact that many older people and some from the manual labor ranks have essentially non-existent or non-usable fingerprints needs to be accommodated as well. The inclusion of all ten fingerprint files and templates onto the card would help to eliminate this problem.
Face recognition will not be acceptable to many in the Muslim religion and is subject to many ACLU concerns. A best "one-to-one" match of the highest reliability requires several views to be stored, increasing template file sixes to the range of 30,000 bytes. While this is no problem when stored on an optical memory card, it is beyond the range of any other ID card to deal with.
Signature, voice, fingers, retina, and other biometrics all have similar weaknesses

In summary, it is our opinion that more than one biometric should be implemented on any secure ID card system, and that the selection of the biometric to be used by any given application at any given time not be known to the cardholder in advance.

This "redundant and random" biometric approach will greatly enhance the overall system security, reduce single vendor dependence, and allow tailoring the system to accommodate all citizens, regardless of their race, religion, age, handicap status, or other limitations relative to a given biometric approach.

It is for the above reasons we recommend the use of two or more biometric elements in any secure ID card system.

ALLOW ROOM TO ADD NEW BIOMETRICS SEAMLESSLY:

Any ID card system storing biometrics in a secure form will have a significant card issuing cost, which means card life and updatability are important. The INS and Department of State optical cards have a 10-year expiration period, more than 5 years beyond any smart "IC" card warranty. This is a long time, and technology will change. The card should be capable of being updated and upgraded in this period, as new biometrics, software, and application requirements come along. This means one of two things—either (1) you have an erasable, changeable media, like a smart "IC" chip card, and live with the risk of changeable and erasable media, or (2) use media
having enough updateable memory, such as the permanent re-

cording media on the optical card, to provide an audit trail to the previous information. This was a key feature for both the INS and the State Department in the selection of the optical card, since it allows them to update the card without the need to re-issue it.

ASSURE OFF-LINE VERIFICATION ABILITY:

Any ID card system should be capable of complete, secure verification of the cardholder to the card without any dependence on a on-line database, although it may be present. The failure of many online systems to be effective, including the INS "INSPASS" program, is their total dependence on a nationwide 100% uptime, on-line database to verify the cardholder ID and allow entry. Most INSPASS system downtime is due to network and communication failures and has constricted the system implementation to less than 100,000 people across the many years the program has been in place.

Having the ability to completely verify the cardholder off-line, using local blacklists in each terminal, would eliminate this problem. Additionally, the off-line capability allows the implementation of mobile and hand-held reader terminals, which can greatly expand the value and usefulness of any ID card system.

PROVIDE FOR SELECTION OF APPROPRIATE BIOMETRIC BASED ON APPLICATION REQUIREMENTS:

Having multiple biometrics on one card means you have the ability to select the most appropriate type for a given situation or application. Using Hand Geometry on doors, face recognition in terminal access points, Iris scan at high security zones, and fingerprints for ticket check in, could all be accomplished seamlessly with one card, optimizing each technology for a given area. The added benefit of this is that the use of multiple biometrics throughout a given system greatly enhances the overall system security, since breaching one biometric does not cause a total system failure. If such a breach is recognized, the system applications could easily be re-programmed to select another card biometric, without the need to re-issue cards. Given the growth of technology and biometrics in general, this is a very important consideration of any new system design.

ASSURE INTEGRITY OF THE BIOMETRIC FILES FROM ISSUER TO USER:

In any system design using biometrics for ID, it is essential to ensure that the biometric file added to the card at the time of issuance cannot be tampered with, erased, or substituted. Without such safeguards in place, there is no security, since anyone can obtain a similar biometric system, create their own biometric template files, and substitute them into the valid ID card. All card systems attempt to minimize this risk, however, only the non-erasable optical memory card can intrinsically eliminate this concern, because the laser writing process, like punching holes in paper, is physically impossible to erase or overwrite.

All Smart "IC" chip cards hold such critical information in their "EEPROM" memory, meaning "Electrically Erasable Programmable Read Only Memory", which means no such assurance can be had. No other card data storage technology, from barcodes to magnetic stripes, is appropriate for secure biometric information that must be updated, yet secure.

SUMMARY

In closing, I would like to point out that the INS and Department of State LaserVisa secure ID cards represent the most advanced biometric card systems in the US, and perhaps the world. The cards have a minimum of three biometric files each, and are vendor independent in their ability to be verified. The card's storage of up to 80,000 bytes of biometric data is ten times more biometric information than available on any other type of ID card, and yet uses less than 20% of the total available card memory.

Other governments are following the lead of the INS. The Italian government has started issuing optical memory-based ID cards as the basis of their new National ID card, and tenders from many other countries are specifying the use of optical memory upon which to base their biometrically secured ID card systems.

Use biometrics for any ID card system. And for full security, flexibility, and long-term system life, the use of more than one biometric on the card is highly recommended.

I will be pleased to answer any questions you may have.

Chairperson FEINSTEIN. Thank you very much, Mr. Haddock.

Miss Lau?

STATEMENT OF JOANNA LAU, CHAIRMAN AND CEO, LAU TECHNOLOGIES, LITTLETOWN, MASSACHUSETTS

Ms. LAU. First, let me thank you for giving us the opportunity to present here. I want to say that it is unfortunate that it often takes a crisis to create an opportunity to make change. About 11 years ago my company was involved with Desert Storm and that certainly brought us a tremendous opportunity during that crisis and also gave us the opportunity to learn about the defense and learn more about technologies, how it could improve our nation.

Well, we are now here at an urgency to really make change because even though we win the war, we are going to create more terrorists around us, so it is important we make change at our borders, as well as what is going on here—not only terrorism, also the most wanted list that could be endangering us domestically, as well.

That being said, let me say that Dr. Atick basically touched on a lot of the basics regarding facial recognitions. I am here to also talk about facial recognition so I am not going to bore you with all the technical data. Let me go straight to the success story.

Again I think a lot of my colleagues have said this is not a test. This is reality. We have spent a lot of money among all of us in this technology to try to improve the nation, so the timing is just right that we have now come here to answer the call. So let me put this to you, some of the success stories, some of the events, some of the installations. And, of course, in my case I will be just talking facial recognition.

In Pinellas County, Florida this year we were funded by the Congress for the sheriff's office to implement facial recognition to assist the jail operations and criminal investigations. Within a couple of weeks we found over hundreds of individuals who are duplicates, with false IDs and what-not, in a total of 350,000 images.

As my colleague pointed out, this is real data. This individual in Pinellas County, it pulls up his face. As you can tell, he has many different looks. He lost weight, he shaved his hair, shaved his beard, and who knows who else he has done to himself but more importantly, he has different identities, he has different names, different Social Security numbers. So we were able to run that and pull him out. As you can tell, he showed up about 15 times.

This is also a system that is currently being piloted at the Department of State to also scrub the database to reduce some of the lists that are not as big as we thought they were.

In the casinos, of course, the casinos has used it for surveillance. Over 100 casinos worldwide have used this facial recognition to scan cheaters, card-counters, and what-not as they walk into the casinos. It became a deterrence for them. They now know to stay away. We have actually found quite a number of cheats at Trump Tower in Atlantic City. It is a fascinating place to go see.

Then access control is another arena and a lot of my colleagues here have talked about access control, getting in and out of places where one belongs to or one should not belong to. We have been active in that for the Department of Defense.

And, of course, the Superbowl has again gotten a lot of attention but that is a tested concept, again that it is possible, although we only identified 19 people but it is enough to save a lot of lives.

In the state of Illinois, it is probably the biggest database we have. It has about 8.5 million images in the database. Every night about 15,000 driver's license applications go into this database and it is searched to see if there is any redundancy or duplicates or false identifications. We currently have learned that the U.S. Marshal has used the Illinois system to confirm information that one of the 15 most wanted fugitives—using the facial recognition, they were able to find Mr. Escabedo's driver's license. From that, they arrested him in Mexico. I think he was a drug trafficker or something like that.

So with that, there is a lot to say about technologies but I urge the Senate to work with industry, to also work with the agencies to make it work for all of us. There is always the barriers to get into agencies, to get them to comply, to work with us. Academia, industry, government could work together and we have proved this over and over again.

We do have another demo here. I am taking a very big chance here. This is a live demo. As you can see the screen, on the right side it is pure white. This is going to make Dr. Atick very panicked now. He is going to say, "Make sure it works, Joanna."

The live screen is where you see the image being captured right now. Carl is not in the database so we will not do anything with him but we did enroll one of your interns. I just wanted to show it to you. I knew nothing about your intern. Ally has been so good.

Chairperson FEINSTEIN. Ally,, what is your problem?

Ms. LAU. So with that, I think I will leave it to the panel to answer questions.

[The prepared statement of Ms. Lau follows:]

STATEMENT OF JOANNA LAU, FOUNDER, LAU TECHNOLOGIES AND VIISAGE TECHNOLOGY

MADAME CHAIRWOMAN AND MEMBERS OF THE COMMITTEE, I want to thank you for the opportunity to testify on the important issue of how biometric technology, and specifically facial recognition technology can be used to prevent persons who wish to carry out acts of terrorism from entering the United States.

As the founder and CEO of Lau Technologies I have devoted the last decade to the use of technology to ensure National Defense. This has led us to create our affiliate, VIISAGE Technology to advance the use of facial recognition technology; a technology that I believe has the potential to fill an important role in this Nation's current border security strategy.

Almost all Americans believe that September 11, 2001 has shown that our borders are not as secure as we once thought that they were. However, it is only by reviewing and changing the current border security measures, as you are doing Madame Chairwoman, that we will be able to move forward and stay abreast with the threats that our Nation now faces. We must admit that there is no single answer, or "silver bullet" to solving our border security issues. Those of us in the private sector must be careful about over-promising or exaggerating "ready made solutions." Clearly, we have tools that can help, one of which I will explain and demonstrate today. Our fellow citizens are demanding better technology and better law enforcement and I am pleased that my company is in a position to contribute. Let me tell you about facial recognition technology.

BACKGROUND ON FACIAL RECOGNITION TECHNOLOGY

Almost a decade ago, researchers at the Massachusetts Institute of Technology (MIT) pioneered a facial recognition method known as "Eigenfaces". Using this technique, any facial image taken from still photographs, live or recorded video or com-

posite sketches, can be enrolled into the "Eigenface" system, which then reduces an individual's face characteristics to 128 coefficients. Once enrolled, and using our algorithm, these images can be compared for possible matches.

Lau Technologies acquired the rights to the MIT technology in 1994. Since that time we have spent millions of dollars and over 100 person-years to build on the original Eiganface algorithm. Today we have 25 patents in place or pending and each face that is compared using our system is subjected to several different algorithms.

From an operational perspective, this software allows law enforcement to compare any face against a digital "mug-shot book" of images in real time to determine if there are possible matches. In the past, it would have taken an indidual hours to manually make this type of comparision with even a few thousand images—In the State of Illinois, we are currenly matching all new driver license applications against a database of 8.4 million existing drivers licenses, to identify fraud and duplicates. Once a search is completed and a gallery is displayed, it is then up to the operator to review the possible matches and determine how to proceed. In this way, facial recogntion technology acts as a powerful force multiplier for investigators.

To date, the technology has been used successfully by Federal, State and local government and the private sector for close to 5 years. Let me give you several examples:

- *Pinellas County, Florid*—This year with funding provided by Congress, the Pinellas County, FL Sheriff's Office began implementing facial recognition to assist with jail operations and criminal investigations.
- *Casino Surveillance*—Our technology is currently being used in over 100 casinos worldwide. These establishments have enhanced their existing cameras with our technology to allow security officers to compare visitors against a database of close to 10,000 known cheats. Since then, the system has identified hundreds of unwanted individuals.
- *Access Control*—today, the United States Army, Navy, Air Force and the Federal Aviation Administration use the technology for access control.
- *NFL Super Bowl*—In cooperation with Federal, State and local law enforcement, our company provided facial recognition technology at last year's Super Bowl in Tampa, FL. Over 60,000 faces were scanned as they entered the stadium and their pictures were compared to a database that included terrorists, fugitives as well as known scalpers and pickpockets. While no one was arrested, 19 probable matches were made using the software. After each comparison that did not result in a match, the individuals image was immediately destroyed.
- *State of Illinois*—Perhaps one of the most successful applications is the 8.4 million drivers license images that are being scanned everyday for duplicates and fraud, which I described earlier. This is by far the largest facial recognition database in the world.

We recently learned that the U.S. Marshals used the Illinois system to confirm information about one of their 15 Most Wanted Fugitives. Using only facial recognition, the Marshals compared a booking photograph of Daniel Escobedo to the DMV database. Within seconds, Mr. Escabedo's driver's license came up first in a database of over 8 million images. The driver's license confirmed information that the Marshals had recently discovered using more traditional investigative techniques, that helped led to Mr. Escabido's arrest.

Since September 11th, we have obviously focused on how we can help ensure the security of our borders. We are working with various Federal Agencies to determine how to best utilize this technology and I wanted to bring to your attention a few applications that we feel could be particularly useful.

VISA ISSUANCE

As you are well aware, last month Ambassador Mary Ryan indicated in testimony before this very Subcommittee that she would like to expand the use of facial recognition technology with the Visa program. We believe an immediate use of facial recognition technology would be the full enrollment and comparison of the State Department's visa database. With an estimated 10 million images already in the database, facial recognition is the only biometric that can compare every individual in this database against every other individual to look for multiple visas under assumed names. In addition, we could immediately run all 10 million images against the FBI and Intelligence community's database of wanted terrorists. Most important to the on-going War on Terrorism, we have the capability to carry out this entire process in less than 90 days.

Going forward, as new visas are issued around the world there will continue to be a need to run these images against the faces of wanted terrorists. In almost every case, the only biometric information that we have about these terrorists is a picture. We would propose that as part of the application process, in addition to the security checks already undertaken, every individual's picture would be compared to the watch-list before a visa is issued.

PORT OF ENTRY SCREENING

After a visa has been issued, we see a further use of facial recognition technology as a method of screening passengers at the Point of Entry. The use of biometric technology for airport security was recently endorsed in the Department of Transportation's Airport Security report. We currently have deployed this surveillance technology at the International airport in Fresno, California and we are in talks with over a dozen additional airports throughout the United States.

In these airports, cameras will be used to quickly capture images of passengers and compare them against the terrorist watch-list. If a match is not made, the passenger's image is immediately destroyed. In the event that a possible match is made, the passenger is further investigated.

SUMMARY

As Congress undertakes the vitally important task of securing our borders, it is clear that biometric technology can play a role. Specifically, if a face is available, and time is limited, facial recognition technology is a valuable tool to further ensure identification and security.

With that, I am available to answer any questions you might have and would be happy to demonstrate for you how the technology works.

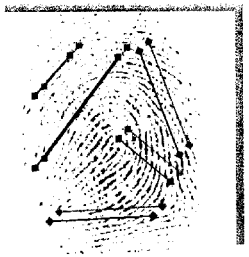
Facial Recognition Experience

- Over 1,500 Lau/Viisage image capture systems are deployed throughout the US.
- Lau/Viisage FR has been chosen by the following:

- TSWG
- United States Army
- United States Navy
- United States Air Force
- U.S. Secret Service
- U.S. State Department
- FAA
- Illinois DMV
- Maryland DMV
- British Columbia DMV
- Pinellas County Sheriff
- Auburn, MA PD
- Prince George County
- Uganda Electoral System
- Over 100 U.S. Casinos
- ATM machines
- HarvardNET Security
- Fresno Airport

Facial Recognition

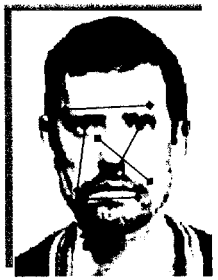
Fingerprints



AFIS for Faces

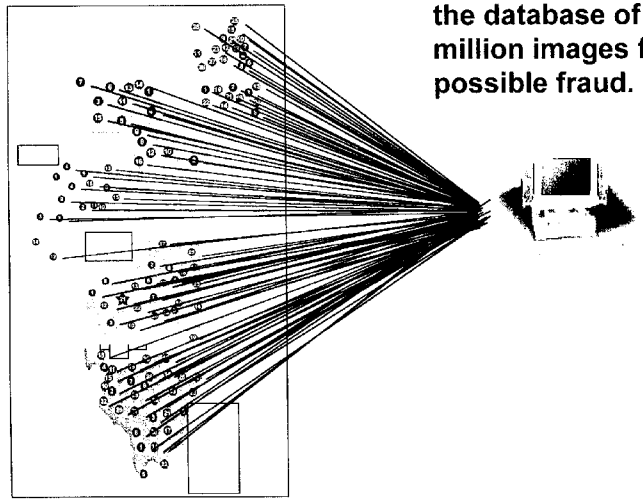
Produces a mathematical value

Facial Recognition

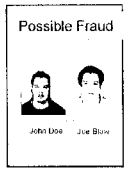


State Of Illinois

Each day over 15,000 new images are captured at 135 Drivers License facilities throughout the State.



Each night new images are sent to headquarters to be compared against the database of over 8 million images for possible fraud.



Each morning State officials review possible matches from the day before.

Match Example

Name: Timothy Pace
ID: 151024
SPN: T0673857
DOB: 06/19/70

Name: Timothy Burdette
ID: 153569
SPN: T0676394
DOB: 03/19/70

Name: Timothy Strickland
ID: 182880
SPN: T0706155
DOB: 06/06/70

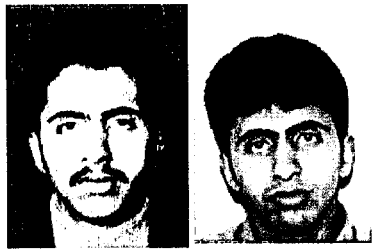
Name: Timothy Williams
ID: 196722
SPN: 0161436
DOB: 04/19/70

Airport Security

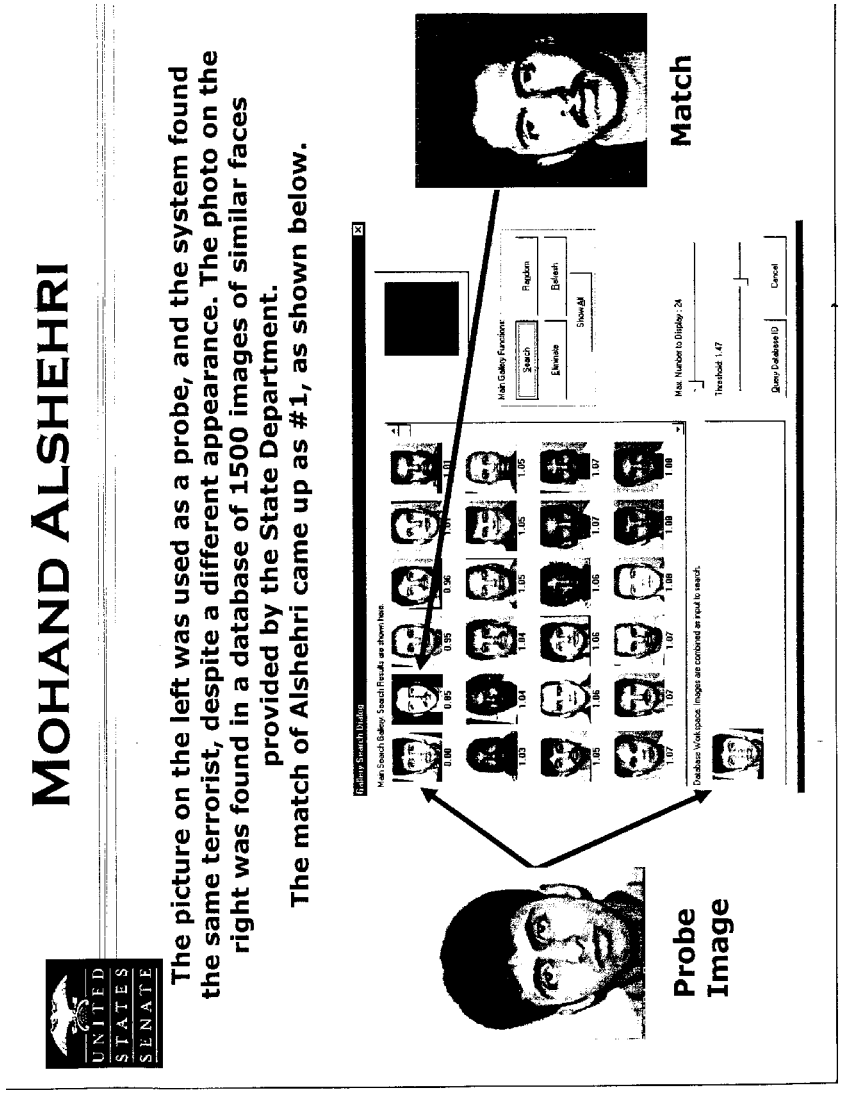
- Strategically located cameras at chokepoints
- Cameras can be overt or covert
- Captured faces are compared to entire database
- Search can be conducted either real-time or after stake-out

Airport Surveillance

MOHAND ALSHEHRI



The FBI released these images, both confirmed as pictures of hijacker Mohand Alshehri, who crashed United Flight 175 into the South Tower of the World Trade Center on September 11.



Chairperson FEINSTEIN. Thank you very much. Thank you. I appreciate all of your testimony. It is a dazzling array of technology.

Senator Kyl, why do you not begin this round?

Senator KYL. Thank you very much.

All of you have been very, very helpful to us and we can see, I am sure, the advantage of each of these systems in different applications.

One question I have, and this applies to a couple of you but let me start with Mr. Haddock and I think it also applies to Miss Lyons. Where you have a card—in fact, let me just take this with the INS because INS uses your card now, as I understand it. Is that correct?

Mr. HADDOCK. That is correct, yes.

Senator KYL. How do you verify that the individual in possession of the card is, in fact, the individual whose data is on the card when that person comes through?

Mr. HADDOCK. At the moment the INS does not do that. The data is on the card that they could do that but they never implemented the readers on the border to do it.

Senator KYL. What would that take?

Mr. HADDOCK. It would take—I have a reader in my briefcase there, a small unit like a CD–ROM drive that could be put on the existing PCs at the border, in any airport. Anywhere the INS has an inspector, they could put this unit on there and it can read the card in a matter of a few seconds.

In the case of the INS card, they put the FBI-quality fingerprint image on it. They intended to select a minutia file to pull from that image to compare against, which can still be done on the existing cards.

Chairperson FEINSTEIN. What is a minutia file?

Mr. HADDOCK. It is the mathematical representation of the picture that actually these technologies match against. They do not match against the entire picture. They pull key points out and make a much smaller file called a minutia file and that is what electronically is matched.

So in the case of the INS file, because these minutia templates, as they are called, are proprietary to the vendors, they did not want to select any given vendor's technology at the offset of this program so they took the whole image with the idea that whenever they wished, they could pull from that image the minutia they needed and it could even be done dynamically even today.

Senator KYL. But it is fine to have the fingerprint on the card. It is a tamper-proof card but it is not a theft-proof card. So I get somebody else's card; I am driving in my car through the port of entry. I show them the card, it is too quick for them to really look at the photo very well and they say okay.

In order to verify that it is, in fact, the person to whom the card was issued, they would have to have the reader there, as well.

Mr. HADDOCK. Absolutely.

Senator KYL. It would take a couple of seconds for that reader?

Mr. HADDOCK. It typically takes about four seconds. When we have shown the INS here is the method to implement it, we show them about a four-second time.

Senator KYL. And how much would that cost for the ports of entry?

Mr. HADDOCK. Today's reader prices, about $2,000 per drive. This is in the quantities—

Senator KYL. $2,000 per machine?

Mr. HADDOCK. Per machine, and that is about the only cost because the rest, you just connect it to the PC.

Senator KYL. And how many machines are there supposed to be?

Mr. HADDOCK. The maximum points would be 3,000. To equip the INS all the way around the country, every back office, front office, would take about 3,000. You could hit obviously the key high-volume points with a lot less. I think probably 85 percent of the

entries come through a few hundred ports so it could be a small amount of money.

Senator KYL. So we need to get at that.

Mr. HADDOCK. I would think so. We have been trying to deliver that message for a number of years.

Senator KYL. I just now got it. Because our time is very short, and we will follow up on that, by the way—where, for example, Mr. Willis, and this applies to Mr. Atick, I think, and others, as well, where you have the facial recognition or the hand you would have to still get the hand of the terrorist or whoever you are seeking to identify into the system somehow the first time, right?

Mr. WILLIS. Right. All of our technologies require enrollment so you know who it is, to be able to compare it with.

Senator KYL. Right. Now contrast that with a photograph. And I guess this is a question to you, Mr. Atick. Do I understand what you were saying is that we have photographs of a lot of these terrorists? They are not necessarily great quality. If you could take the photograph with your own machine what would the percentage be of identification?

Mr. ATICK. The studies that were done in England regarding the effectiveness of facial recognition shows you that it is as effective as the best fingerprint technology if you could do the enrollment yourself using the controls that the system requires. But the point that I made in my testimony is that even with the FBI's database that is just taken in the field from surveillance cameras and covert operations, we can still give you a value, that 60 to 90 percent of these terrorists will be intercepted.

Senator KYL. Right. Thank you.

Chairperson FEINSTEIN. Sixty to—

Mr. ATICK. Sixty to 90 percent, according to some recent studies that were done over the last two months.

Senator KYL. Just one other thing with regard to the hand. You said that the facial does not change over the aging process?

Mr. ATICK. The geometry.

Senator KYL. The aging process or through attempts at modifying the visual appearance. The hand changes over time. It can get very arthritic, for example. I happen to know that. And it looks a whole lot different at age 60 than it did at age 20.

Mr. HUDDART. If I can answer that?

Senator KYL. Yes, please.

Mr. HUDDART. Our template is adaptive so that every time you use the device it is looking for small changes that might occur, for example, in pregnant women whose hands tend to swell or over a longer period of time, the arthritic condition you mentioned. So the template adapts every time you use the device. We are looking for small changes and it will adapt for that.

Senator KYL. Okay. Rather than take the whole time here let me turn it back to you, Senator Feinstein.

Chairperson FEINSTEIN. Just very quickly, what is clear to me is that you are going to have to have a combination of technologies to really do it right.

Secondly, the other problem is it looks like there is going to be a kind of—I don't want to use the word hodge-podge but a lot of different technologies. Everybody is competing in this field. How do

we get the standards that develop the combinations that can be the most widely used with an eventual aim of having sort of the worldwide database with other countries entering into it? Anybody have any thoughts?

Ms. LAU. I would comment that if you were to do today, for example, if you were to do just one or two or six airports, it is not going to solve the problem.

Chairperson FEINSTEIN. Right.

Ms. LAU. You have to deploy it universally to really solve the problem. We are really in this war to fight terrorists. I think our allies will have to work with us. Individuals were asked, the two officials here, regarding sharing databases with Interpol. I do not think this is acceptable. From a citizen's standpoint I think that if we are in this together, why could not our policy be such that we could share the database? That is one thing.

True, there are a lot of technologies in place but not one single technology is going to provide your silver bullet. And the other thing is that every application and environment is very different and we rely on some of the experts that you have working in your government to work with industry. We are here to offer our expertise and help but we are not taking over their job. We have to work with them.

Chairperson FEINSTEIN. See, one of my concerns is whether we do have the expertise that is necessary. I think in a way, the INS example is classic and my experience with government has been, whether it is local government or now national government, there really is not the level of expertise that exists in the private sector, for obvious reasons. You know, we do not pay our people as well as the private sector does. Most of the hottest people go into the private sector.

So absent this kind of consortium—we get very informal in these Subcommittees meetings, Senator Kyl—absent the ability to develop the standard and have the private-public partnership that is effective, I am not sure we will ever get at it. I am frankly appalled that INS would do a system whereby you have one half of the system and all these people have their cards and the other half is not in place.

Mr. HADDOCK. To give the INS some credit, the card brought with it anti-counterfeiting features which stopped their main concern, which was counterfeiting on the street corner. The previous paper pink cards that were in issue were widely counterfeited. They needed to stop that immediately. By implementing the optical card, putting the etched image of the person on it, they effectively stopped that immediately.

Chairperson FEINSTEIN. Are you saying that the counterfeit business is out of business? Because I do not believe it is.

Mr. HADDOCK. The previous card was a laminated pink piece of paper which anybody could make. The problem is they left them out there. They are still there. They are still valid for another six years, this previous generation, very easy to defraud cards. I asked the INS two weeks ago, "Can't you do something about that?" and they said they cannot do it; Congress has to do it. Somebody has to tell them to recall these cards.

The Department of State did. For the border-crossing cards with Mexico, they stopped those. They stopped them on September 30. They no longer accept the paper previous generation cards. But the INS still takes the old generation, the pink cards, and so forth, and no one is doing anything about that. No one even talks about it.

Senator KYL. If I could just add to that, I think it is because they have not completed the issuance of the tamper-proof cards yet.

Mr. HADDOCK. But the cards have a 10-year life so the pink ones are just slowly trickling in, so it will take another five years before you really have a tamper-proof card, unless someone says to do it today.

Ms. LYONS. Excuse me. If I might add?

Chairperson FEINSTEIN. Go right ahead.

Ms. LYONS. For what it is worth.

I think the point that Mr. Haddock made in terms of it is a combination of biometrics that might be most appropriate—the point that you made at the beginning of the hearing in terms of a consortium is necessary, I absolutely think it is. We can create the expertise that we need to make the decisions. Even this panel, experts that we are, we have a blind spot as it relates to the other technologies.

So I do think that it is a consortium that needs to come together to make those decisions. To balance, if you are talking widespread, you know, you probably want a technology that has been honed, is reliable, and is inexpensive. In more critical areas, facial may be more appropriate in some areas. So I think together we have to conclude those decisions.

Mr. Haddock, his view of the reader cost, these readers today, when plugged into an existing computer system, run around 20 bucks. That is how the technology has gone down in price relative to some of this technology. It has been around for a while and price has now come way down and these door devices are less than $1,000 today.

Mr. HUDDART. If I can comment, too, on that question?

Chairperson FEINSTEIN. Yes.

Mr. HUDDART. There are several pockets of government agencies that already have significant experience with biometrics—Sandia National Labs, for example. The FAA have done a lot of work, also. So I think if we could draw from that experience that have used a lot of the products represented here, the industry association, which myself and Dr. Atick are on the board. The International Biometrics Industry Association has proposed the national biometric security project, which would take those best practices and in an unbiased fashion make recommendations for applications and further testing.

But if I could also say that while that is all important to do, the fact remains that, for example, San Francisco airport is safer today because it has already done something and my concern is that we spend two years developing standards and we are not any more secure than we are today. There are proven systems represented here that can address those concerns.

Chairperson FEINSTEIN. I must tell you when I was mayor I told the director of the airports that if there is ever a bomb out of San Francisco, do not show up the next day because you do not have

a job. And at that time there were even bogus bomb dogs, so they got the message and really went to work and, I think, produced.

But what we have here, you are all rugged individualists. You are all obviously extraordinarily bright. Could you put together to Senator Kyl and myself a kind of, if you would, quick compendium of what we would have to do to have the kind of system standardization that is necessary? Does that make sense? Because the result of this hearing, for me, is we have some wonderful things out there but it is such a dazzling array, it is very hard for lay people to know what works better in what kind of situation. And because you are all individualists, you all have different companies and it would be very useful if you could come together and say we think these are the imperatives that you need to have to move forward.

Mr. HADDOCK. If I could answer that briefly, there is an international standards working group on international travel documents, WG–3, and in that there is a machine-readable data segment which allows each type of data element that is encoded on a card to be read by any other reader so that people could know whether it had a hand or an eye or an iris or whatever, by reading it.

So you could have multiple biometrics, the cards could be different, they could be used for different applications, but there is a standard to help sort that out. So there is some sense to all this.

Mr. WILLIS. Madam Chairman, there is also some cooperation amongst the panel here already. We have been working together to look at—

Chairperson FEINSTEIN. Would you excuse me just for a minute? I have a meeting with the prime minister of Mongolia. He has just arrived. So I am going to have to leave but I am going to turn this hearing—and thank you very much—and turn it over to the very able hands of Senator Kyl, if I might.

Senator KYL. Thank you. I am already late, as well.

Please finish and then—

Mr. WILLIS. What I want to say is I think we are as sensitive as an industry as you are to the solutions and we have been informally having discussions on making a tool set. When you are trying to make a solution you need a tool or a set of tools based on what you are trying to solve and I think we are starting that informally and I think this would certainly help expedite that.

Senator KYL. One final thing. I should announce that the record will be open until November 21 at 5 p.m., which means that each of you who would like to submit any additional testimony or information may do so. I will try to get my questions, if there are any more, to you well in advance of that.

I just did have one final question. Are any of you suggesting that any of the data that goes into these cards be data on an Internet system or do each of you agree that these need to be discrete systems separate from the Internet?

Mr. ATICK. They need to be networked at the end of the day.

Senator KYL. They need to be networked?

Mr. ATICK. They need to be networked if they are to give you the power of controlling access and the power of scalability. But obviously that produces a whole slew of issues associated with the privacy and security of that data.

Senator KYL. It produces a whole slew of issues with me, so that is something we have to talk about.

Mr. ATICK. Absolutely.

Mr. HADDOCK. We think it should be completely decentralized, off-line, secure on the card.

Senator KYL. Yes, that is my inclination. So could I ask all of you to maybe just submit us a little memo reflecting your thoughts on that particular question? I know there are pros and cons of both. I have my prejudices but would appreciate being edified by the opinions of each of you.

Thank you again. This was a very, very helpful hearing. We appreciate all of you being here. The hearing is adjourned.

[Whereupon, at 12:04 p.m., the Subcommittee was adjourned.]

[Submissions for the record follow.]

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

SUBMISSIONS FOR THE RECORD

Senator Dianne Feinstein and Senator Jon Kyl

"VISA ENTRY REFORM ACT OF 2001"

STRENGTHENING COUNTERTERRORISM EFFORTS AT THE PORTS OF ENTRY

The legislation to strengthen counterterrorism efforts at the ports of entry will do the following:

Section 1: Short title. "Visa Entry Reform Act of 2001."

Section 2: Establishment of a Comprehensive "Lookout" Database

Mandate the creation of a comprehensive, integrated "lookout" database of visa holders and other nonU.S. citizens who enter the U.S. Require all immigration, intelligence, and law enforcement agencies to contribute relevant information, and the require the database to be accessible at all ports of entry. Centralized data system must be flexible and scalable to meet ongoing immigration and law enforcement needs in the future.

Direct the Homeland Defense Director to oversee the development of the database in conjunction with the Department of Justice, the INS, Department of State, Department of Transportation, CIA, and private industry, to identify and track terrorists and suspected terrorists.

Require the database to be designed to connect law enforcement, intelligence, INS and State Department information in one centralized data system so that information may be readily shared among agencies.

Require the Director to submit report to Congress within 3 months of enactment regarding the type of data contained in centralized database; levels of access to such data; methods to secure such data from abuse and/or unlawful access; and infrastructure needs to implement system through national and overseas offices of relevant Federal agencies.

Require the INS to upgrade its electronic data system to include biometric data (i.e., fingerprints, photographs, facial recognition technology) on all foreign nationals applying to enter the U.S. within 6 months.

Require the INS to place into a centralized data base all foreign nationals who have violated the terms of their visas (e.g., remained in U.S. after visa expired, committed a crime, performed unauthorized work or took unauthorized classes).

Not later than 30 days of enactment, require the Secretary of State to establish within each U.S. embassy a terrorist lookout committee.

Section 3: Implementation of a New Biometric "SmartVisa"

Require the INS and State Department to establish a biometric "smart visa" to enable the INS to track foreign nationals upon entering and exiting the U.S.

Authorize funding for biometric card readers and scanners to be deployed at all U.S. land, air and sea ports of entry to implement process.

Section 4: Reform of the Visa Waiver Program

Mandate that within 1 year, countries wishing to participate in the visa waiver program first provide a tamper-resistant, machine-readable passports.

Within 2 years, all countries must also include biometric data on those passports, which conforms to U.S. standards.

The Attorney General and the Secretary of State shall jointly determine standard biometric identifier(s) that would be required on all U.S. and foreign passports and visas.

Mandate that the INS check all Visa Waiver passport numbers, names, and, where available, biometric data with the new, centralized database.

Require participating countries to report stolen passports to the State Department.

Section 5: Pre-Screening of Foreign Nationals Prior to Arrival in the U.S.

Repeal Sec. 286(g) of the Immigration and Nationality Act, which requires that all in-transit flights to the U.S. be cleared by the INS within 45 minutes.

Require all nonimmigrants to submit fingerprints and/or other designated biometric data to the State Department when applying for a visa.

Require the State Department to electronically transmit versions of its visa files to the centralized lookout database, so that information on arriving aliens is available to the INS prior to the time of inspection.

Access to database shall be limited to authorized immigration and law enforcement personnel. Require the Attorney General and Secretary of State to develop regulations specifying the limitations of use.

New and increased penalties for the misuse or theft of information contained in database.

Section 6: Passenger Manifest Information

Require all airlines, cruise lines, vessels and cross-border bus lines submit passenger and crew manifests to the central database prior to departure.

Require the INS to check passenger information against the lookout list.

Section 7: Requirements for Federal Documents

Mandate that all U.S. Federal identification documents be fraud- and tamper-resistant.

Mandate that all immigration related documents, including work authorization and visas, be fraud- and tamper-resistant, contain biometric data, and, if applicable, include the visa's expiration date.

Where minimum Federal standards apply to state commercial licenses, those standards are amended to require that such documents and licenses:

provide positive identification of the holder;
are tamper- and fraud-resistant; and
contains biometric data.

Any person conferring a personal identity document on an unauthorized basis would be in violation of Federal law.

Section 8: Bar on Entry of Foreign Students from Terrorist-sponsoring countries

Prohibit the State Department from issuing student visas to individuals from countries included on the Department's list of terrorist-sponsoring states.

Permit the Secretary of State to waive the bar on student visa issuance for a foreign student if he performs an extensive background check and certifies that the student does not pose a threat to the national security.

Section 9: Reform of the Foreign Student Visa Process

Require any additional costs to fully implement and expand the tracking program established under Sec. 641(a) of the Illegal Immigration Reform and Immigrant Reform Act. [8 U.S.C. 1372a]—beyond that covered by Congressional appropriations—to be covered by application fees paid by foreign students.

Prohibit educational institutions from providing INS Form 1–20 to foreign nationals applying for foreign student visas.

Require educational institutions to submit the INS Form I–20 directly to the Department of State. The form must provide:

a. the identity of the student;
b. the student's address in the country of origin;
c. names and addresses of parents and siblings;
d. contacts in country of residence, including organization affiliations, or close associates who could verify information about the student;
list of prior work experience;

f. academic course of study at institution;
g. period of enrollment at the institution; and
h. the consulate at which the foreign national will apply for a student visa.

Require the State Department to notify the school at which the alien intends to enroll upon the issuance of a foreign student visa.

Require all such data to be entered into the centralized database established under Sec. 1.

Require the INS to conduct a background check prior to the issuance of a foreign student visa, which would include, but not be limited to:

a. a name check, and biometric data check where available, on the INS lookout system, the INS IDENT system, the Interagency Border Inspection System; and the FBI's IAFIS system; and
b. a check to ensure that the alien is not subject to a bar to reentry as a result of a previous violation of immigration law.

Require all educational institutions to submit data to the INS within 30 days of the foreign student's enrollment, including:

a. the student's full name;
b. address in country of origin;
c. actual address in the U.S.;
e. date of commencement of studies;
f. degree program and list of courses;
g. status of student (e.g., full-time or part-time); and
h. date of the last day of classes.

Require schools to provide the INS status report on a quarterly basis to:

a. certify that the student has enrolled and registered; and
b. notify authorities of any disciplinary or law enforcement action involving the foreign student.

Require all schools to immediately report to the INS within 30 days:

a. the failure of a student to register, enroll or appear at designated institution;
b. the foreign student's withdrawal from the institution; and
c. any failure to comply with the terms of his or her visa.

Require the INS to notify the State Department and immigration authorities when foreign students fail to meet the requirements of their visas. Require the INS to enter relevant data regarding the students' immigration violations in the central database.

Prohibit the automatic extension of a foreign student visa. Foreign nationals must apply for an extension of their student visas and submit to second background check. Students who have violated the terms of their visa while in the U.S. would not be eligible for an extension and would be immediately deportable.

Modifies current definition of an "approved institution of higher definition" under the current law to include vocational, trade, flight training and language training schools. This effectively expands the list of schools and type of foreign students the INS is required to track.

Section 10. Requirements Relating to the Admission of Nonimmigrant Aliens

Require all nonimmigrant visa applicants to submit to fingerprinting and/or other biometric requirements to enable the INS and State Department to perform extensive background checks on individuals before they enter the U.S.

Require the Secretary of State to assign such additional number of consular officers as may be necessary to achieve effective screening of visa applicants. Authorizes such sums as necessary.

Require the INS to perform a background check before the State Department can issue a visa. Authorize such sums as necessary.

Section 11. Additional Port of Entry PerSOnneL

Authorize an increase of not less than 200 INS inspectors in each of the fiscal years 2002 through 2006.

Authorize an increase in INS investigatory personnel for the purposes of identifying and locating visa violators, particularly those who pose a risk to national security.

Authorize an increase of not less than 200 U.S. Customs inspectors in each of the fiscal years 2002 through 2006.

Section 12. General Accounting Office Study.

Requires a study on the feasibility of implementing a plan wherein nonimmigrants are required to present to the Commissioner each year to provide cer-

tain status information. Requires GAO to report within 1 year on the findings of the study.

Statement of Hon. Strom Thurmond, a U.S. Senator from the State of South Carolina

Madam Chairwoman:

I am pleased that this Committee is considering the use of biometric identifiers in the war against terrorism. Biometric identifiers, including fingerprints and photographs, have national security implications because they would make the forgery of identification documents more difficult. Visas and immigrationrelated documents should contain these identifiers, which will make it harder for terrorists who enter the country to conceal their true identities. Biometric identifiers should also be added to a comprehensive database that would include information about all noncitizens entering the United States. These safety measures would assist immigration officials in identifying terrorists who attempt to cross our borders.

While I recognize that most aliens are law-abiding people who make valuable contributions to our society, it is apparent that there are some who wish to do us harm. The colleagues.

The bill would require aliens to present a SmartVisa upon entry into or exit from the United States. This is a good start. However, I would like to extend the SmartVisa system beyond entry and exit purposes. We should require that aliens use the SmartVisa card when applying for jobs -and registering for courses. By swiping the SmartVisa, employers and educational institutions would be alerted to the expiration of a visa or the withdrawal from classes by an alien on a student visa.

The use of biometric data and the careful monitoring of aliens is especially necessary in light of the large number of immigrant and nonimmigrant visas granted each year to people from terrorist-supporting countries. In Fiscal Year 2000, we issued more than 3,000 visas to aliens from Iraq and more than 5,000 to people from Sudan. Almost 16,000 visas were issued to aliens from Syria and more than 30,000 were issued to people from Iran. We also annually admit individuals from terrorist-supporting states such as Libya, Cuba, and North Korea. Because of the large numbers of people who obtain visas from states that support terrorism, it is critical to our National security that we monitor alien activity inside our borders.

Beyond the use of SmartVisas, I believe that we should take further steps to protect the American people. In light of the recent terrorist activity within our borders, Congress should consider the annual registration of aliens. Annual registration was required in the past but was discontinued in 1981. Currently, aliens are required to notify the Attorney General of changes in an address but are not required to update information on a yearly basis.

The Federal Government has the power and the responsibility to verify that aliens are in the country for authorized reasons. At the least, annual registration should be required for nonimmigrants, most of whom will not become U.S. citizens. Annual registration of nonimmigrants would help the government to monitor the movements and activities of aliens who hold work and study visas. It is important to note that according to media reports, one of the hijackers of September 11 arrived in the United States on a student visa but did not attend classes.

Madam Chairwoman, thank you for holding this hearing on a timely and important topic. The use of biometric data on a SmartVisa System and the development of a centralized database would be very beneficial to the fight against terrorism. If used in conjunction with annual registration, I believe that the Federal Government would have the tools necessary to ensure that terrorists do not take advantage of our open society to murder more Americans. In this fight against terrorism, it is essential that we use the newest technology feasible, and biometric data is a step in the right direction. The use of biometric data will assist immigration officials in determining whether an alien is a threat to the safety of Americans. We should not miss out on this opportunity to make our country safer and more secure.

RAND
ARLINGTON, VA 22202–5050
November 14, 2001

The Hon.Dianne Feinstein, Chairwoman
Subcommittee on Technology, Terrorism and Government Information
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairwoman Feinstein:

Thank you for asking me to submit written testimony for your subcommittee's hearing on "Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism." I am honored by this consideration. As my written testimony, I am submitting Biometrics: Facing Up to Terrorism, RAND Issue Paper (IP-218) published this year.

To help protect RAND's legal responsibilities, please include the following information with the written testimony: "John D. Woodward, Jr. is a senior policy analyst at RAND. He has testified on biometrics before the U.S. Congress and the Commission on Online Child Protection. RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. This testimony is based on a variety of sources, including research conducted at RAND. However, the opinions and conclusions expressed are those of the author and should not be interpreted as representing those of RAND or any of the agencies or others sponsoring its research."

If you have any questions or require additional information, please contact me at (703) 413-1100, extension 5242. Thank you again for your invitation.

Sincerely yours,

JOHN D. WOODWARD, JR., ESQ.

○