S. Hrg. 107–1113

FUTURE OF AIRPORT SECURITY— DYNAMIC NEW TECHNOLOGIES

FIELD HEARING

BEFORE THE

SUBCOMMITTEE ON AVIATION

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

NOVEMBER 5, 2001

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE
90–128 PDF WASHINGTON : 2005

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

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia
BARBARA BOXER, California
JOHN EDWARDS, North Carolina
JEAN CARNAHAN, Missouri
BILL NELSON, Florida

JOHN McCAIN, Arizona
TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia

Kevin D. Kayes, *Democratic Staff Director*
Moses Boyd, *Democratic Chief Counsel*
Mark Buse, *Republican Staff Director*
Jeanne Bumpus, *Republican General Counsel*

SUBCOMMITTEE ON AVIATION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
JOHN B. BREAUX, Louisiana
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia
JOHN EDWARDS, North Carolina
JEAN CARNAHAN, Missouri
BILL NELSON, Florida

KAY BAILEY HUTCHISON, Texas
TED STEVENS, Alaska
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
OLYMPIA J. SNOWE, Maine
SAM BROWNBACK, Kansas
GORDON SMITH, Oregon
PETER G. FITZGERALD, Illinois
JOHN ENSIGN, Nevada

CONTENTS

WITNESSES

APPENDIX

FUTURE OF AIRPORT SECURITY— DYNAMIC NEW TECHNOLOGIES

MONDAY, NOVEMBER 5, 2001

U.S. SENATE,
SUBCOMMITTEE ON AVIATION,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Morgantown, WV.

The Subcommittee met, pursuant to notice, at 12 p.m., in courtroom 165, West Virginia University College of Law, Law Center—Evansdale Campus, Hon. John D. Rockefeller IV, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, U.S. SENATOR FROM WEST VIRGINIA

Senator ROCKEFELLER. I want to thank everybody for being here. I would like to start off with a statement, as Chip and Jane Garvey know, we sometimes do in Congress. Thank you very much for being here. Thanks very much for being with the only university in the country that offers undergraduate degrees in something that we're going to be talking about. I want to thank President Hardesty and the university for making this opportunity available to us, for hosting what is a meeting of the Senate Aviation Subcommittee, which I have the honor to chair, for this very important hearing on technologies that can be deployed to improve our aviation security situation, which is obviously a matter of overwhelming importance.

For years, the State of West Virginia, and West Virginia University in particular, have been quietly establishing themselves as a leader in perhaps the most promising of security technologies, so-called biometrics or human identification devices. West Virginia University houses the Center for Identification Technology Research, which is a university/industry cooperative research center under the auspices of the National Science Foundation. I think most West Virginians would not necessarily know that, but it is true, and it is profoundly important.

West Virginia is home to the U.S. Army's Biometrics Fusion Center in Bridgeport, West Virginia, and throughout the region there are a number of related security companies, some of which have participated in the impressive technology expo, which I hope you have all had a chance to see, and will be continuing during the afternoon outside of this room.

Many of our witnesses, including most especially one of my favorite Americans, FAA Administrator Jane Garvey, have traveled quite a ways to be here. You all have. I think you will find the surroundings here and the people here very much relevant to your work.

We in Congress have spent the last 6 weeks working to improve security at airports. That should not come as a surprise. Unfortunately, the House of Representatives last week rejected the far-reaching aggressive bill put forward by the subcommittee in the Senate that I serve on, and by the full Senate by a vote of 100-to–0 and passed, as I say, unanimously.

This, to be honest, is a real setback for security from my point of view and I think from any reasonable point of view. But if we all keep the safety of the American people first in our minds, I'm sure that in the conference committee, which I think will start on Wednesday, that we will be able to reach some kind of an agreement and get aviation security at work in the airports as soon as possible. Because changes since September 11 have not been that dramatic, particularly in the smaller airports.

In the meantime, we have to begin to explore the role that technology can play in addressing security challenges. Prior to September 11, our best intelligence sources believed that a terrorist attack using airplanes as missiles and airports as launching pads was something that was associated with Hollywood movies, but certainly nothing more than that. And certainly not worth spending millions and, more to the point, maybe billions of Federal dollars to prevent such a scenario from taking place.

Now, obviously, all of that has changed and changed forever. Today, we have to think much more comprehensively and much more creatively than we have in the past. And there is a lot of instinct within us as Americans—not because we are not afraid of the future, but there is a great instinct in America now to hold on to what it is we have been doing, and our way of doing business. And the whole concept of making changes and trying out things which are new, putting in concept two ideas or an idea which may bring in some conflicting aspect to it, all this is something that generally we try to avoid when we're in a peacetime situation.

Well, we are not. We are in a war on the international level, and some would argue that we are in a modified war on a domestic level also. So we have to be able to monitor and to share in real time information about who is getting on a plane, what are they bringing with them, who has access to airport security areas and also to aircraft, and ultimately whether all of those people really are who they claim to be.

Last Tuesday, Secretary Mineta was quoted as saying that "an unacceptable number of deficiencies continue to occur at the Nation's airports." And he's quite correct. Appropriately, and very rightly, in my view, he expressed a willingness to ground aircraft, to ground them again and close entire concourses of major airports if the situation does not improve. Hence, the pressure on the Congress to pass legislation which can begin to be implemented and which gathers the confidence of the American people so they'll get back on airplanes.

Technology in the hands of well-trained, highly skilled professionals who are accountable should allow us to address these problems. And we must address them as quickly as possible if we're going to restore that confidence to the traveling public and the financial health to an industry which we suddenly have discovered is a Behemoth of an economic factor in our American economic life; that is, the airline industry.

[The prepared statement of Senator Rockefeller follows:]

PREPARED STATEMENT OF HON. JOHN D. ROCKEFELLER IV,
U.S. SENATOR FROM WEST VIRGINIA

Good morning. First, I want to thank President Hardesty and West Virginia University for hosting this hearing. I also want to express my appreciation to Jane Garvey and the other witnesses for coming to West Virginia today. West Virginia is on the cutting edge of technology that is critical to making major security improvements that we all recognize must be put into place immediately. Administrator Garvey will not only have an opportunity to talk about the challenges we all face, but also learn what West Virginia can offer to the Nation's security.

As many of you know, we have spent the last month trying to figure out how to improve security at airports. Jane Garvey has been leading the way for the Administration. The attacks of 9/11 were not a failure of the FAA. The FAA controllers throughout this country and the flight crews did a remarkable job rerouting and landing all of the planes across the entire Nation. The controllers in New York that watched and listened to the attack in horror also must be commended. Prior to 9/11, everyone was searching for explosive devices being placed onboard a plane. Today, we want to know who is getting on a plane, who has access to airport security areas and aircraft, and if they do—are those people who they claim to be? Technology can be deployed to answer these questions.

Last Tuesday, Secretary Mineta stated that "an unacceptable number of deficiencies continue to occur" at the Nation's airports, threatening to close entire concourses if necessary. Technology, in the hands of well-trained, highly skilled, professionals, can address these concerns.

Airport security is a multi-layered process. Airports, for example, are responsible for the airport perimeter and the facility. Air carriers today are responsible for screening passengers and baggage.

Focusing first on the airport—every airport has a series of doors that provide access for airport and air carrier personnel. Airports also have different types of gates that limit access for catering trucks and other vehicles. No one wants anyone without a legitimate reason to have access to baggage areas, catering services, or airplanes. Technology can tell us who should have access and close those doors to prevent unauthorized access.

Focusing on passenger screening—we want to know who is getting on planes, and are those people who they say they are. Currently, security screening begins at check-in. All passengers are questioned to determine if a dangerous item has been passed to them unknowingly. Additionally, computer-assisted passenger prescreening (CAPPS) software uses classified criteria to identify certain "selectees" for more intense scrutiny.

If a passenger checks baggage, it may be screened for explosives using x-ray equipment, but the availability, use and cost of this equipment are all problems that need to be addressed. To protect against bombings, the positive passenger-bag matching (PPBM) procedure matches passengers and their bags. Bags whose owners do not actually board the aircraft are removed.

The most visible part of the screening process is the security checkpoint—where passengers and their carry-on bags are screened. Passengers themselves walk through metal detectors, and carry-on bags are screened by equipment that displays an x-ray image of the bag contents. Operators who see suspicious objects in the image hand search bags as a backup procedure.

We need to ensure that security information is available on a real-time basis. Prior to 9/11, we were headed for gridlock at airports throughout the country. Now, we are looking for people to fly, but that will change and we must have systems in place that can expedite passenger processing or long lines will be the norm, and not the exception.

There are a number of technologies that we know can be deployed. We want these technologies deployed today so that we can positively identify people getting onboard planes and track persons obtaining access to sensitive areas. Specifically, we will examine the role of biometrics and other related technologies.

This is a national problem and we in West Virginia want to help solve it. The State of West Virginia is in the forefront of biometrics technology. WVU houses the Center for Identification Technology Research, a National Science Foundation University/Industry Cooperative Research Center and we are home to the U.S. Army's

Biometrics Fusion Center. In addition, several security product companies are based in West Virginia.

Our first panel will set the stage and indicate the role technology can play in airport security. The FAA has been concerned about unauthorized access for years. The American Association of Airport Executives and the Air Transport Association have long advocated greater emphasis on security and understand the advantages of biometrics and related technologies. The International Biometrics Industry Association will describe how the industry is meeting this challenge. WVU will describe the State's participation in the biometrics field. Honeywell and EDS will give us the industry perspective.

I cannot overemphasize how important this hearing is. We are trying to address a problem that is widely recognized, not only by the aviation security community but also by the public. Our economy depends on air travel. The country must be assured that air travel is safe. Until we are able to convince people that previous holes in security have been fixed, they will continue to be reluctant to commit themselves with the same level of confidence as before the events of 9/11.

Our first panel will set the stage and give us a sense of the activities underway at the FAA, the airports, and among the major airlines to improve security and to deploy available technologies.

The FAA, embodied by Jane Garvey, has been concerned about unauthorized access for years without a great deal of public support or private support. And the FAA has a new task force focusing on security research and development and can give us a sense of the financial commitment that we need to make as a Nation to deploy security technologies throughout the system.

The American Association of Airport Executives, which is Chip Barclay, and the Air Transportation Association—and in terms of the whole security aspect of it, the top guy is Mr. Doubrava—have long advocated greater emphasis on security. The airport professionals all do that. And they understand the practical advantages of biometrics and related technologies.

On the second panel, we will focus on the security technology industry itself and related research. The International Biometrics Industry Association, West Virginia University, Honeywell, and EDS will tell us both what's possible today and what's in the works for deployment in the future.

And with that, let me invite Administrator Garvey to begin our testimony today. And thank you for being here.

STATEMENT OF HON. JANE F. GARVEY, ADMINISTRATOR, FEDERAL AVIATION ADMINISTRATION

Ms. GARVEY. Thank you very much, Mr. Chairman, and it is a real pleasure to be here this morning. And I want to echo your statements about the president of this university. We are really delighted to be here, and I know when you asked us to attend, you spoke so enthusiastically about the wonderful work the university does in biometrics. And we are just delighted to be here, a number of us from the FAA, to see that firsthand. So we appreciate the opportunity to be with you this afternoon.

I'd like to begin by talking a bit about what we've done with the wonderful support we've seen from Congress—in your committee in particular, Mr. Chairman—over the last several years. You've invested about $440 million, and that's been money, I think, that's been absolutely critical in the area of security. It's been used to purchase and deploy explosive detection systems, explosive trace detection devices, and threat image projection like x-ray machines.

Certainly, in the days and in the weeks ahead, we will be working very closely with the Congress to complete action on our budget for the next fiscal year. Certainly, I think that, particularly after the days of September 11, the role of technology will be a significant factor in the development of any new aviation security bill. And we certainly look forward to working with you and other members of the committee as you prepare to go to Congress. As you know, there are two manufacturers of certified EDS products, and that's a really important technology.

Senator ROCKEFELLER. EDS?

Ms. GARVEY. Explosive detection systems. So that's an important technology for us. One of the manufacturers, as you may know, had some operational difficulty. But we are very encouraged by improvements that the vendor has made to the software and the hardware. And this week, for example, we have a team of IG inspectors as well as FAA inspectors who are in Dallas/Fort Worth assessing those improvements. We really want to see competition out there. So having EDS manufacturers who are certified and with equipment that works well is very important to us. We're pleased to see some improvement for that manufacturer.

We are also aggressively pursuing other technologies that need to be deployed. For example, we have three vendors under a grant program at our task center developing a smaller version of EDS, and that, I think, is very promising for some of the smaller regional airports. And we're working with them to move their schedules forward. They're just in the early stages, and we'd like to see them aggressively move those schedules forward.

Like many Members of Congress, we've received thousands of ideas and suggestions since September 11. In response to one of the recommendations made by the Rapid Response Team convened by Secretary Mineta, we were tasked to work 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.

On October 25, we had our first meeting, our first security research and advisory committee. And I might add that these are made up of experts from universities, experts from manufacturing companies, from Boeing, from NASA; really from both across government and in the academic world. The committee will evaluate over a thousand recommendations that have been made to the FAA.

I've asked for a report of initial short-term recommendations by the end of this month so we will have a sense of what can be deployed quickly by the end of this month. And then we've also asked that the advisory committee provide a report to identify promising longer-term technology, and I will look forward to the discussions later in the afternoon from some of the other panelists who have some information on other technologies.

In addition, we're sponsoring our third international aviation security technologies symposium in Atlantic City later this month. The symposium will be important in helping to identify those technologies that can help meet the challenges we face.

I think it's important to know that aside from the technologies that are certified by the FAA, there are a variety of technologies currently available either if an individual air carrier or an individual airport wants to use them. Some of those technologies I know are going to be on display here, and I am very eager to see them at the close of this session.

We know, for example, that the airport in Charlotte, North Carolina has tested and has evaluated iris recognition as a means to verify airport personnel. We understand that was a very successful pilot program that they ran.

Chicago and San Francisco are similarly testing hand and fingerprint technology for employee verification. We certainly think that this whole area of biometrics is very promising, exceedingly important, and we really are encouraging folks to pursue that even more aggressively.

Some of the technologies hold great promise, but they also pose some significant challenges for all of us. Our goal, certainly, is 100 percent screening of all passengers, baggage, and airport and airline personnel. Certainly it will require an increased level of commitment by the entire industry, certainly by Congress, by the airlines, by airports, and by the American public.

Mr. Chairman, again I want to thank you for having us here today, and we look forward to working with you and the Subcommittee as we move forward on what is an absolutely critical and important issue. Thank you.

[The prepared statement of Ms. Garvey follows:]

PREPARED STATEMENT OF HON. JANE F. GARVEY, ADMINISTRATOR, FEDERAL AVIATION ADMINISTRATION

Chairman Rockefeller, Senator McCain, 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 the aftermath of the tragedy that occurred on September 11, the Federal Aviation Administration (FAA), like the rest of the government, is rethinking how we approach 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 take a moment to discuss our most recent initiatives to ensure that all viable security technologies 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.

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 our security goals. This committee will evaluate over 1,000 recommendations made to the FAA by various industry sources. I have asked that the committee provide me with a report on its initial recommendations by the end of November. I expect 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.

In addition to the efforts of the advisory committee, the FAA is 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 to identifying those technologies that can help meet the challenges we face in our approach to aviation security.

With that said, I would like to provide a broader overview of our efforts to enhance security through technology. The goal of aviation security is to prevent harm to aircraft, passengers, and crew, as well as support national security and counterterrorism 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 planned to spend an additional $97.5 million.

One-hundred-fifty 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 the methods of passenger selection are non-discriminatory. 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. Eight-hundred-nineteen ETD devices have been installed in 175 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 checkpoints to improve screener vigilance and training. To date, 732 of these units have been deployed to 71 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, they must use it. We are working hard to ensure that carriers and airports that now want these systems will be able to obtain them, but to date it has been more expedient to encourage their use than to mandate their use by regulation. 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. Iris and fingerprint identification technologies are currently being tested in the operational environment. The Rapid Response Team recently 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.

Just to make sure that we are not missing anything that is out there, FAA issued an announcement that appears on our web site 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 and I 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. Last week, Secretary Mineta directed FAA special agents to crack down on airport and air carrier security deficiencies by taking decisive steps including clearing concourses, re-screening 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 with the help of its national and international partners, that 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 the means of attack and must be able to anticipate future risk to the civil aviation environment. In a democracy, there is always a balance between 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.

Senator ROCKEFELLER. Thank you, Administrator Garvey. We're very grateful to you for, in what must be an unbelievably hectic schedule, taking your time to come here. It is very important.

Mr. Charles Barclay, as I indicated, is President of the American Association of Airport Executives. We welcome you. His nickname is Chip. I have to call him that because I do not know how to say Charles. But we are very glad you are here.

STATEMENT OF CHARLES M. BARCLAY, PRESIDENT, AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

Mr. BARCLAY. Thank you, Mr. Chairman. I appreciate the opportunity to be here as well and want to begin by thanking you and your very professional staff for all their help getting the security bill done in the Senate. We look forward to getting the bill done as well in the conference.

And we also appreciate the response for the small communities, both the air service issues and, now more recently, the reimbursement of the security costs since September 11. It is a really major issue in the smaller communities, and we appreciate your leadership on that.

Since September 11, we all know that we have got to do a better job in three areas. We've got to put more security on airplanes. But more importantly, to try to keep bad things from happening in the air, we have to provide a better perimeter around parked aircraft, which is a big part of my members' jobs. And we have to apply a more professional screening process for both passengers and baggage. And that is what I would like to talk about in terms of technology.

But first I'd like to say that technology is very important for getting greater security, but it's also important for getting convenience back into the system. If we continue to have 2-hour lines at airports on each end of a business trip, that makes a 1-day business trip totally impractical in our system. The economics won't work if we don't get that convenience, together with security, back in the system. The only way we can process 700 million passengers and 2 billion bags is to do a better job of applying technology for our security concerns. The screening process is not really my members' part, but we think it's a critical element of getting back to that convenient system and getting more security. There are three ways you can really use technology in screening people and baggage. One, you can look for bad people with facial recognition; with better matching of lists that's been talked about from various security agencies; and with a variety of other ways. We can look for bad things with the EDS machines Jane was talking about: X-rays and body scans. While there's some great technology out there, it is still very hard to find a needle in a haystack when you're dealing with 700 million people.

Senator ROCKEFELLER. And that's just the United States?

Mr. BARCLAY. Just in the U.S. The third way is to let non-threats identify themselves. In fact, technology works well when we interview someone once and allow that person to get a voluntary smart credential. We were talking about the terminology we used on the Rapid Response Team. It's not a travel card, it's just a credential. If you ask people to give us a lot of information once and a biometric, you can then use that positive identification to determine who is not a risk and screen these people quickly while you apply most of your intensive resources on people you don't know anything about who are coming into the system. So people would still have an option to get the smart credential, a heavy investigation once, then get greater convenience every time you fly.

If you're uncomfortable with giving information or you're not in the group you want to treat as low risk, then you're going to get a different process at the airport and get much greater intensity in screening you and your bags. And that is also a way to really have a threat assessment to know where we should apply our resources first while we're ramping up this new security system.

The other part that's more directly affecting my members is employee background verification and using that information to make sure that the right people are on the ramps and around the perimeters of airplanes while they're parked. We strongly support Administrator Garvey's call to get all employees who have access to secure areas full criminal history checks. It's done here in West Virginia, as a matter of fact. We need to get those criminal history record checks and get them done quickly. She said that that needs to be done within 9 months. We are strong supporters of that.

We're also doing the best we can to help the FAA. We think it's very important to have a copy of that raw data that also comes in here to the FBI so the airports can use that database for all the people that are cleared. You want to use that over and over again. Rather than just having a card swipe and a PIN to access the name, you have a card swipe and a biometric, either a fingerprint or iris recognition. A number of the other biometric technologies can be very good for making sure we've got the people that we know and we've checked out having access to parked airplanes.

So one of the points that I'd like to leave you with is that we do need to put greater security and convenience back into the system. I would also like to make the point that there are really two threats to our system right now, and either one could shut it down. One of those threats is that we don't do enough in adding security to get public confidence back so that we get all the people back flying who should be. The danger is that you won't have enough people on the airplane.

The other danger that we have in front of us is moving too quickly in so many areas and trying to apply so much technology at once that we bottleneck the system and don't put enough people on airplanes. That can also bring the system down and feed into the goal that the terrorists had on September 11.

So we think we need to add technology. We need to do it smart. We need to approach the highest threats first as we get these new systems in place, and at the same time, keep air transportation running in the United States.

Thank you very much for having me here. It's been a real pleasure.

[The prepared statement of Mr. Barclay follows:]

Prepared Statement of Charles M. Barclay, President, American Association of Airport Executives

Chairman Rockefeller and Members of the Senate Commerce Subcommittee on Aviation, thank you for inviting me to participate in the hearing today on aviation security. I am testifying today on behalf of the American Association of Airport Executives (AAAE). AAAE represents the men and women who manage the primary, commercial service, reliever and general aviation airports. I appreciate this opportunity to discuss ways that we can use new technology to improve aviation security.

The tragedy of September 11 has changed air transportation forever. We never designed our aviation security system to withstand a threat from teams of special operations-type forces, comprised of suicide pilots, trained for years, with the goal of using the plane as a bomb. It is still hard to believe such people exist, but now that we know they do, airport and aircraft security must be hardened to defend against this and other potential threats that, in the past, we would have labeled as unreasonable. A military-type threat requires a near-military defense. This job would be easier if we could focus on security alone, but we cannot. Changes must both increase security and permit aviation to operate efficiently as public transportation.

Airports, airlines and general aviation must begin to plug the security holes, one by one, despite the complexity, cost and daunting magnitude of the job. While the costs and complexities are huge, they pale in comparison to the greatest threat to our system's future. The 800-pound gorilla of problems is today's lack of public confidence in air transportation safety, and the concomitant revenue impact that attitude has on all aviation businesses. Surveys released at the end of October showed only one-third of the public have a high level of confidence in aviation security. Our industry cannot survive and perform its essential economic role unless we turn that perception around—and soon.

Air transportation is the safest form of transport in history. More people have traveled farther and more safely by air than any other system invented. Yet, we still cannot expect the system to regain the broad public confidence lost on September 11 until we make significant, systemic improvements in security. I do not believe the public demands an unachievable "perfection" in air travel, but they are demanding more security onboard the aircraft, more professional screening of passengers and baggage and better perimeter control around parked aircraft.

The Administration, airlines, airports, and Congress are already taking the necessary first steps to improve aviation security. Immediately after the terrorist attacks occurred on September 11, the Federal Aviation Administration (FAA) closed our nation's commercial airspace system and issued two emergency amendments that included several security initiatives. As all of you know, airports and airlines were required to implement these new security measures before the FAA allowed them to resume their operations. Airports, for instance, were immediately required to deploy more law enforcement officials and K-9 units, increase security inspections throughout their facilities, strengthen access control measures and remove all vehicles parked near their terminal buildings.

With the possibility of additional terrorist attacks in the United States, the Administration has taken additional actions to improve aviation security. The President announced his decision to deploy National Guard personnel to about 420 airports nationwide, and the FAA issued additional emergency amendments requiring airports to implement even more security measures. Last week, Secretary of Transportation Norm Mineta said the FAA also plans to crack down on security screening failures at airports around the country and consider re-screening passengers, emptying concourses and holding flights if necessary.

Congress is also taking legislative steps to improve aviation security and restore public confidence in our aviation system. The Senate Commerce Committee, under the guidance of Chairman Hollings, Ranking Member McCain, Aviation Subcommittee Chairman Rockefeller and Ranking Member Hutchison, drafted a bipartisan bill that the Senate unanimously approved just 1 month after the terrorist attacks. The fact that Committee members and staff were able to draft an aviation security bill and usher it through the Senate in only a few weeks is a testament to your hard work and dedication. All of you deserve to be commended for the leadership you have provided in the past several weeks.

Much of the debate that has occurred in Congress on aviation security has focused on those responsible for screening passengers and their carry-on baggage, cockpit security and Federal air marshals. In light of the hijackings that occurred in September, it is now more important than ever that we improve the training, testing, and the proficiency of those individuals conducting the screening of passengers and baggage. Hiring competent screeners, strengthening cockpit security and deploying more Federal air marshals will certainly help improve aviation security. These actions may solve part of the problem, but we must use new technology to ensure that the hijackings and terrorist attacks that occurred on September 11 will not happen ever again.

Just a few days after the terrorist attacks, Secretary Mineta formed two teams to examine ways to improve airport and aircraft security. I served on the Rapid Response Team on Airport Security, which issued its report on October 1. We concluded that new technologies must be deployed more widely to augment aviation security and that there is an urgent need to issue "smart credentials" to facilitate expediting the processing of passengers. I think there are many new technology options that Congress and the Administration should explore in an effort to enhance security at our nation's airports. The Senate Commerce Committee included several new technology provisions in the Senate-passed aviation security bill, and I would like to take a moment to outline a few other proposals for your consideration.

Technology can be effectively used in three ways: (1) to find dangerous "things;" (2) to find dangerous people; or (3) to verify the identity of people who do not present a risk. The first two are relatively difficult even with good technology due to the large number of people and bags being processed in air transportation—they amount to finding the proverbial needle in a haystack. The third, however, is relatively easy with today's technology as long as we come to agreement on the criteria of a low-risk profile, and it makes the haystack smaller for application one and two.

USE SMART CREDENTIALS TO IDENTIFY PASSENGERS

At the top of my technology list is a "smart credential" as called for in the Rapid Response Team report. We cannot run an efficient public transportation system if we try to treat all 700 million passengers a year like potential terrorists. We need a voluntary system that allows frequent travelers to provide enough information on themselves, so government and industry can agree they belong in a "low-risk" pool.

In return, a so-called "smart card" with biometrics can confirm identity and provide access to an expedited screening process. The system can then concentrate its resources for rigorous screening on passengers who do not qualify to be listed as "low-risk," or passengers we do not know anything about (including those individuals simply uncomfortable with providing information on themselves).

Such a voluntary database of passengers can reside either in or out of government control, but the Federal Government must be involved in validating the criteria for information used in this process. I think smart credentials are key to identifying those who may be potential threats to aviation security, and I am pleased that the aviation security bill passed by the Senate calls for the Department of Transportation (DOT) to study options for improving positive identification of passengers including the use of biometrics and smart cards.

DEPLOY EXPLOSIVE DETECTION SYSTEMS AT MORE AIRPORTS

There are many innovative technologies that make it easier for screeners to identify explosives and other dangerous weapons. While these systems are commonly viewed as only as effective as the trained personnel who operate them, they are an increasingly essential facet of the aviation security equation. The integration of a new generation of Explosive Detection Systems (EDS), as called for by the 1996 Presidential Commission on Aviation Security and Terrorism, has been an important addition to our efforts to improve the security of our aviation system.

As with any new technology, planning and training are critical to realizing the potential of explosive and other weapons detection systems. Today, forty-six airports around the country are using new generation explosive detection systems. These and other new technologies must be integrated into the nation's airports at a much quicker pace and with increased attention to the resources, training and infrastructure requirements necessary for their effective use.

USE NEW TECHNOLOGY TO TIGHTEN ACCESS TO SECURE AREAS IN AND AROUND AIRPORT TERMINALS

In addition to improving the screening process for passengers and baggage, we need to do a better job of controlling access to secure areas in and around airport terminals. Last year, the DOT Inspector General highlighted the shortcomings in access control technology and procedures at some airports around the country. Airport operators take this issue seriously, and we need to continue to improve procedures and deploy new technology to tighten the perimeter of secure areas. It is critical that we use new technology such biometrics and smart cards to control these access points. However, we should be aimed at developing a universal database to all airport and airline employees with secure area access, rather than airport-by-airport individual databases.

USE BIOMETRIC FINGERPRINT TECHNOLOGY TO EXPEDITE CRIMINAL HISTORY RECORD CHECKS

Just as we need to have well-trained screeners, we must also focus on eliminating undesirable behavior that can nullify even the best technology used to control secure areas. Toward that goal, it is essential that we concentrate our efforts on ensuring that only those persons who have undergone thorough criminal history record checks are granted access to secure areas.

Last year, Senator Hutchison introduced S. 2440, the Airport Security Improvement Act of 2000. Like many on this Committee, we strongly supported that legislation because it called on the FAA to work with air carriers and airport operators to strengthen procedures to prevent unauthorized access to secure areas of airports and commercial aircraft. The bill, which was enacted into law last year, requires criminal history record checks for new security screeners and others who have access to secure areas in the top 20 most at risk airports. The legislation requires criminal history record checks for new employees at other airports to be phased-in over 3 years. It also requires the FAA to expand and accelerate the Electronic Fingerprint Transmission Pilot program.

Administrator Garvey recently announced that the FAA will order criminal history record checks on all workers who have access to secure areas of airports and commercial aircraft now rather than phasing those checks in over the next few years. The Senate Commerce Committee also included a provision in the Senate-passed aviation security bill that would require criminal history record checks within 9 months. Since airports, airlines and vendors employ approximately 600,000 to 750,000 people, airports will need electronic fingerprint assessment technology to expedite these criminal history record checks. Only a small number of airports currently have biometric fingerprint systems to speed criminal history checks. Once airports submit these fingerprints electronically to the Federal Bureau of Investigation (FBI), it is imperative that the agency have the necessary resources to conduct their background checks in timely manner.

After the FBI conducts a criminal history record check on a potential new employee, airports are limited in their ability to disqualify that person by a very specific list of criminal convictions. That list, which airports use to determine who is allowed access to secure areas at airports, should be broadened to include other criminal convictions and other acts that may pose a threat to aviation security. Since various Federal agencies such as the U.S. Customs Service keep records of persons with a propensity to commit criminal acts and or terrorism, airports should be able to submit the name of potential new employees to a single entity to determine whether that person is on one of those Federal watch lists. Further, airports should have the option to go beyond the Federal requirements and perform background or criminal history checks on any airport employee.

EXPLOIT OTHER BREAKTHROUGH TECHNOLOGIES

As I mentioned previously, the Rapid Response Team on Airport Security concluded that new technologies must be deployed more widely to augment aviation security. Specifically, we recommended that the FAA establish an Aviation Security Technology Consortium to identify and test new security-related technologies at our Nation's airports. We also recommended that the Department of Defense expedited the review of classified technologies with potential application to aviation security with a view to identifying and, consistent with national security requirements, declassifying applications likely to be of value.

DISSEMINATE INTELLIGENCE TO A DESIGNATED AIRPORT SECURITY COORDINATOR

New technology requires good intelligence. The FBI, Central Intelligence Agency and other intelligence agencies each play their own part in monitoring, identifying and assessing threats to national security. Some of the information processed by the intelligence community identifies potential threats to the safety of civil aviation, and intelligence officials share some of this information with offices in the DOT and FAA. However, very little of this critical data is shared with the front line airport and airline personnel responsible for implementing security procedures.

Aviation security needs to be among the top priorities of the intelligence agencies responsible for identifying terrorist threats. Coordination of intelligence dissemination with the Secretary's Office of Intelligence and Security, appropriate FAA staff and finally airport security coordinators will dramatically increase the likelihood that real threats to the system are met with real local response and preparedness.

As a direct result of the recommendations from the 1996 Presidential Commission on Aviation Safety and Security, aviation security consortia were formed and vested with the authority to work cooperatively with Federal regulators to meet the goals of increased aviation security. This increase in the level of effective communication and cooperation has steadily improved the baseline of aviation security. With the events that occurred last week, this type of government and industry cooperation is particularly important. Airport security professionals play a key role in developing, implementing and maintaining effective security measures, and their input should be used as we develop new ways to increase aviation security.

Mr. Chairman, I would like to make one final point. As we discuss ways to use new technology to improve aviation security in the future, I hope we will not lose sight of the fact that airports are taking a number of steps to improve aviation security right now. Those Federal mandates, which I described earlier in my testimony, have resulted in significant cost increases for the nation's airports. These new security requirements are important to our efforts to enhance aviation security and absolutely necessary given the horrific events that occurred in September.

Although the Senate-passed aviation security bill authorizes funds to reimburse airports for their new security costs, it unfortunately does not include the necessary appropriations. I hope Members of the Senate Commerce Committee will work to ensure that airports in their respective states and throughout the country receive the reimbursement they need to comply with the new security initiatives imposed by the FAA. As you move forward later this week and next to the conference on the aviation security bills passed by the House and Senate, we look forward to working with you and your talented staff to craft a final product that enhances the security at airports and airlines across the country and instills the confidence in the American traveling public to fly in the safest, most secure system in the world.

Chairman Rockefeller and members of the Senate Commerce Committee Subcommittee on Aviation, thank you again for inviting me to participate in the hearing today on aviation security. All of us at AAAE look forward to working with you and others in the aviation industry during the days and weeks ahead on ways we can use new technology to enhance aviation security.

Senator ROCKEFELLER. Thank you, Chip.

Our third witness is Mr. Richard Doubrava, who is the Managing Director of Security for the Air Transport Association. You're an expert, and I look forward to hearing from you.

STATEMENT OF RICHARD J. DOUBRAVA, MANAGING DIRECTOR, AIR TRANSPORT ASSOCIATION

Mr. DOUBRAVA. Thank you, Senator Rockefeller. On behalf of the Air Transport Association and our member carriers, I'd like to thank you for the opportunity to participate in this important meeting hosted by the West Virginia University.

Senator ROCKEFELLER. Can you turn that mike up a little closer to you?

Mr. DOUBRAVA. Representing an industry that is absolutely reliant on the development and application of new technologies, we take special interest in the subject matter under discussion today.

Since the tragic events of September 11, the industry, in concert with the Federal Government, has undertaken a number of steps to enhance aviation security.

Recent Congressional passage of antiterrorism legislation in association with the pending House-Senate conference to reconcile differing approaches to Federalize the aviation security screening programs, are moving us closer to a more national approach to homeland security.

Let me also commend you, Senator, for your leadership in these vital areas by your service on the Senate Committee on Commerce, Science, and Transportation in the U.S. Senate as well.

As we move forward as a Nation to determine the outlines of our homeland security, technology will play an important part in the efforts to enhance the Nation's security baseline.

Our challenge is to deploy technology in a sound and rationalized way while also recognizing that no single technology nor security procedure can provide a foolproof security system. The public expects an aviation security system that effectively deploys a variety of technology applications and operating procedures capable of addressing all vulnerabilities. This system must also be adaptable in order to adjust to varying and changing threats.

For purposes of our discussion today, I shall focus on some of the immediate goals of the industry which will depend greatly on the application of appropriate technologies.

Computer assisted screening which permits the application of technology and associated procedures on identified individuals is the central component of any effective aviation security system and our efforts to protect the traveling public from terrorism. Such a system must be rigorous and have the full array of intelligence resources available to filter individuals under the protection and oversight of our national government.

It is not enough to focus on searching for threat items; we must refocus our attention on those individuals that threaten our national and aviation security. Here the government must utilize the latest in technology applications to collect, harmonize, and process all necessary data to scan and identify passengers for whom additional security scrutiny is necessary.

Another area where appropriate technology can benefit the aviation security process is the creation of a voluntary program to permit the use of a universal travel card using a "smart card" approach by travelers after having appropriate background checks completed and verified. The program would greatly enhance the current airport security process by permitting designated "precleared" individuals to utilize enhanced security processes based on their completed security background checks. Fingerprint technology and other forms of biometric devices could be used to support such a program.

Another area of concern is the ability to prevent unauthorized access to secure airport and air carrier areas by limiting access to only those individuals permitted to be in such areas. We believe that current technology can be utilized to confirm and verify the identity of such personnel throughout the operational and secure areas of the airport environment.

We believe that the Federal Government should determine the necessary parameters of such a program to deploy it on a national basis. We do not want to repeat the hodgepodge approach taken in the late 1980s and early 1990s to the Airport Security Access Program. The important intent of this program was undermined by a location-by-location approach that did not meet the needs of the air carriers for standardization and dramatically increased industry costs. Further, this would give additional confidence to the public in an area of repeated expressed concern.

Such programs could be readily expanded to include flight crews, law enforcement officers, and other specific entities needing to move through the national aviation system. Funding for such a program must be allocated on a Federal basis as part of our Nation's homeland security efforts.

Failure to do so will leave the industry and the airport community dependent on limited resources and multiple approaches which undermine the intent and integrity of such a system.

For purposes of brevity, I will not address the challenges of passenger, baggage, and cargo screening. The industry is committed to working with Congress and the Administration in these complex areas. These issues will continue to be a major focus as we move forward together to find solutions to these complicated technology issues.

I do want you and the Subcommittee to know that the air carriers are working closely with Secretary Mineta and Administrator Garvey in aggressively pursuing solutions to some of these challenges. We are actively participating in finalizing recommendations of the special Rapid Response Teams created after the tragic events of 9/11, and are certain that many of them will be implemented in the timeframe set out by the President and Secretary Mineta.

We also commend FAA Administrator Garvey for her active efforts and constructive approach with the airline industry in the days since September 11. Under her direction, a special task team has been created to identify and review every available aviation security technology to determine what areas within the aviation environment could benefit from such applications. I am honored to participate in this effort, and look forward to casting a wide net for new ideas and approaches to aviation security.

Senator Rockefeller, in closing, let me summarize a few of our thoughts. Our Nation is involved in a complex and challenging war against those who seek to terrorize and murder innocent Americans for their own distorted personal goals.

Civil aviation is a primary target for such actions since it reflects the ability of people and ideas to move freely throughout the world. Such freedom of movement and thought is a threat to these dark forces of hate and terror. It is incumbent upon our national government to move quickly and judiciously to strengthen aviation security and make it a national priority—not just today, but in the weeks, months, and years ahead.

We stand ready to work with you and your colleagues in the Congress and the Administration to accomplish this task. Through our combined efforts and commitments, we are more likely to prevent future acts of aviation terrorism and reassure the American people that our system is as safe and secure as we can make it.

I would be pleased to respond to any questions you might have at this time.

[The prepared statement of Mr. Doubrava follows:]

PREPARED STATEMENT OF RICHARD J. DOUBRAVA, MANAGING DIRECTOR, AIR TRANSPORT ASSOCIATION

Senator Rockefeller, on behalf of the Air Transport Association and its member airlines,[1] I would like to thank you for the opportunity to participate in this important hearing here in Morgantown, West Virginia.

Representing an industry that is absolutely reliant on the development and application of new technologies, we take special interest in the subject under discussion today.

Since the tragic events of September 11, the industry, in concert with the Federal Government, has undertaken a number of steps to enhance aviation security. These include:

- Installation of new security devices to strengthen cockpit doors on nearly 100 percent of aircraft fleet.
- Implementation of a domestic Federal Air Marshal (FAM) program.
- Expansion of CAPPs screening program to 100 percent of all passengers and coordination with Federal agency watchlists.
- Deployment of the National Guard troops to the nation's airports.
- Revalidation of air carrier employee identification media and match against FBI watchlist.
- Additional and Ongoing Security Enhancements to the FAA air carrier and airport programs.

Further, recent Congressional passage of anti-terrorism legislation in association with the pending House-Senate conference to reconcile differing approaches to Federalize the aviation security screening program are moving us closer to a more national approach to "homeland" security. Let me also commend you Senator Rockefeller for your leadership in these vital areas by your service on the Senate Committee on Commerce, Science and Transportation and in the U.S. Senate as well.

Our members believe that a unified Federal security program utilizing the government's resources and expertise including a strong intelligence capability is critical to enhancing aviation security. In addition, a standardized approach to air carrier and airport security programs will further strengthen these efforts as well. At the heart of these efforts is the subject of your hearing today—"Dynamic New Technologies."

As we move forward as a Nation to determine the outlines of our "Homeland Security", technology will play an important part in efforts to enhance the nation's security baseline. Our challenge is to deploy technology in a sound and rationalized way while also recognizing that no single technology nor security procedure can pro-

[1] Airborne Express, Alaska Airlines, Aloha Airlines, America West Airlines, American Airlines, American Trans Air, Atlas Air, Continental Airlines, Delta Air Lines, DHL Airways, Emery Worldwide, Evergreen International Airlines, FedEx Corporation, Hawaiian Airlines, JetBlue Airlines, Midwest Express Airlines, Northwest Airlines, Polar Air Cargo, Southwest Airlines United Airlines, United Parcel Service Airlines, US Airways.

vide a foolproof security system. The public expects an aviation security system that effectively deploys a variety of technology applications and operating procedures capable of addressing all vulnerabilities. This system must also be adaptable in order to adjust to varying and changing threats.

For purposes of our discussion today, I shall focus on some of the immediate goals of industry which will depend greatly on the application of appropriate technologies.

Computer assisted screening which permits the application of technology and associated procedures on identified individuals is the central component of any effective aviation security system and our efforts to protect the traveling public from terrorism. Such a system must be rigorous and have the full array of intelligence resources available to filter individuals under the protection and oversight of our national government.

Only a unified Federal approach reaching across the jurisdictional lines of the FBI, CIA, INS, U.S. Customs and other agencies will succeed. Congress and the Administration will need to address the outstanding appropriate legal issues to insure that such a program is applied in a fair, but rigorous manner. It is not enough to focus on searching for threat items; we must refocus our attention on those individuals that threaten our national and aviation security.

Here the government must utilize the latest in technology applications to collect, harmonize and process all necessary data to scan and identify passengers for whom additional security scrutiny is necessary.

Another area where appropriate technologies can benefit the aviation security process is creation of a voluntary program to permit the use of a universal travel card using a "smart card" approach by travelers after having appropriate background checks completed and verified. This process would greatly enhance the current airport security process by permitting designated "pre-cleared" individuals to utilize enhanced security processes based on their completed security background checks. Fingerprint technology and other forms of biometric devices could be utilized to support such a program.

This could be accomplished by the use of a variety of technologies readily available which are secure and tamper-proof. Clearly, the current security clearance process in place at our nation's airports since the tragic events of 9/11 could be greatly enhanced by eliminating the need to treat every passenger as a high risk individual. Our security program should focus efforts on those that could pose a threat to aviation security readily identify and expedite those known not to be such.

Another area of concern is the ability to prevent unauthorized access to secure airport and air carrier areas by limiting access to only those individuals permitted to be in such areas. We believe that current technology can be utilized to confirm and verify the identify of such personnel throughout the operational and secure areas of the airport environment.

We believe that the Federal Government should determine the necessary perimeters of such a program and deploy it on a national basis. We do not want to repeat the hodgepodge approach taken in the late 1980s and early 1990s to the Airport Security Access Program. The important intent of this program was undermined by a location-by-location approach that did not meet the needs of the air carriers for standardization and dramatically increased industry costs. Further, this would give additional confidence to the public in an area of repeated expressed concern.

Such programs could be readily expanded to include flight crews, law enforcement officers and other specific entities needing to move through the national aviation system. Funding for such a program must be allocated on a Federal basis as part of our nation's "homeland security" efforts. Failure to do so will leave the industry and airport community dependent on limited resources and multiple approaches which undermine the intent and integrity of such a system.

For purposes of brevity, I will not address the challenges of passenger, baggage and cargo screening. The industry is committed to working with the Congress, and the Administration in these complex areas. These issues will continue to be a major focus as we move forward together to find solutions to these complicated technology issues.

I do want you and the Committee to know that the air carriers are working closely with Secretary Mineta and Administrator Garvey in aggressively pursuing solutions to some of these challenges. We are actively participating in finalizing recommendations of the special Rapid Response Teams created after the tragic events of 9/11 and are certain that many of them will be implemented in the timeframe set out by the President and Secretary Mineta.

We also commend FAA Administrator Garvey for her active efforts and constructive approach with the airline industry in the days since September 11. Under her direction, a special task team has been created to identify and review every available aviation security technology to determine what areas within the aviation environment could benefits from such applications. I am honored to participate in this effort and look forward to casting a wide net for new ideas and approaches to aviation security.

Senator Rockefeller, in closing let me just summarize a couple of thoughts. Our Nation is involved in a complex and challenging war against those that seek to terrorize and murder innocent Americans for their own distorted personal goals. Civil aviation is a primary target for such actions since it reflects the ability of people and ideas to move freely throughout the world. Such freedom of movement and thought is a threat to these dark forces of hate and terror. It is incumbent upon our national government to move quickly and judiciously to strengthen aviation security and make it a national priority—not just today, but in the weeks, months and years ahead.

We stand ready to work with you and your colleagues in the Congress and the Administration to accomplish this task. Through our combined efforts and commitment we are more likely to prevent fixture acts of aviation terrorism and reassure the American people that our system is as safe and secure as we can make it.

I would be pleased to respond to any questions you might have at this time.

Senator ROCKEFELLER. Thank you very much, Dick.

Administrator Garvey, let me just—or to all of you, pose a philosophical question. When people listen to your testimony and they hear a lot of technology, goes along with thinking about the future, people say, now, wait a second. You know, this is the way my life has been. And somebody starts messing around with that, that gets into my privacy and that begins to upset my life, and I don't like that. And then without necessarily thinking about the whole broad picture, some people would say, well, I don't want to make those changes. And what I'd like to do is just—when I took off from Washington last night and flew to Pittsburgh, I was selected out at random.

Ms. GARVEY. Our system is working.

[Laughter.]

Senator ROCKEFELLER. It was about time it happened. And I was really gone through, which I was very happy about. I thanked people—not under bated breath, but I thanked them all the way through that they were doing it.

Now, what got me through in all cases was this. It is my Senate identification card. United States Senator J. Rockefeller. And oh, by the way, this was given to me 17 years ago when I was in the Senate. Now, my question is—this could be forged. It isn't, but it could be. And, you know, life has changed. So why is it that the American public can hear about words like smart card or biometrics or all kinds of things which imply a different way of doing things—you know, a 2-hour waiting line—although those can be cut down in length if we do the right things—inconvenience, change of lifestyle, ways of doing things, putting off business travel.

Why is it that, in your view, people should be able to think at least as much about their own personal security and the security of their friends and children and country people as well as the inconvenience and the so-called invasion of privacy? I mean, we're facing that on the Internet. We are facing that everywhere. But as soon as you say "invasion of privacy," people start backing off from what could be very intelligent solutions to make their lives much safer. How do we deal with that problem?

Ms. GARVEY. Well, this is—and Chip and I were talking about this coming down. I think one way to deal with it is, first of all, on a voluntary basis. Here, for example, we were thinking about airport security, and Chip spoke about the real challenges about having a safe system, but not having it so inconvenient that people won't travel. So if it were voluntarily, first and foremost, to get a card that is a smart card—as Chip said, give more information—and if you do that and if you're part of that system, then you can be processed through in a more efficient way. I think that might be one way to begin so that people become more comfortable with it.

And I certainly acknowledge the challenges that are there. You don't want to take it so far that you really do invade people's privacy. But I've also been struck in talking with people at airports—and I've done a lot of that lately—that people are willing to sacrifice some of those issues that in the past maybe were considered very sacred. And they'll say, "You know what? I'm really concerned about my security now, and I would be willing to perhaps answer questions that I might not have been asked—might not have wanted to answer in the past."

So I think voluntarily is the first way to begin to give people a level of comfort and also to see that it really can work. And then I think a constant re-examining of the privacy issues, because I think they can be solved. They're not easy, but I think they can be solved.

Mr. BARCLAY. I think there is public confusion because we've talked about both mandatory and voluntary systems, and an awful lot of people start talking about mandatory systems, which we do need for employees and you might consider for foreign nationals or people on visas or people you think are a higher threat of some kind.

But the bulk of those 700 million people can be handled well. Look at all of us who belong to frequent flyer programs, where we voluntarily give away lots of information on ourselves in return for benefits, including convenience.

We need to separate the notion of mandatory systems, which employees are going to have to put up with, from the voluntary pool database that doesn't even have to reside in government. It could reside in industry, because it's voluntary. Government's got to be part of it because they've got to agree we're collecting the right factors and criteria that allow you to identify someone as a low risk or a non-threat to the system.

But we should give people a choice, like they have at the grocery store. Fewer than seven security threats come through this line here. If we don't know anything about you and you have a basketfull of security threats, you're going to go through the slower line and you're going to get much more rigorous screening. And that's particularly important in the early days when we have limited resources and we have to keep things moving. You've got to figure out how to get at those highest threat folks first.

The CAPPS system is currently making that attempt. I think the Chicago incident of this weekend is a good story about CAPPS, because it caught that person, and it got them more vigorous screening. And that's where the items he had on him were discovered.

So we've got to figure out ways to apply technology to reduce the threat. If you want to find a needle in a haystack, start with a small haystack. And we can reduce the size of the haystack we're searching with other technologies like facial recognition and matching up names and things. We can also make that haystack smaller by letting all of us who are willing to volunteer to do so. And then our only technology challenge is verifying you've got Barclay every time it says that's Barclay coming through. Technology is great for doing that.

Mr. DOUBRAVA. Senator, I agree. I think the challenge for us is, first of all, to make the process as streamlined as possible for those individuals that decide they want to be in the voluntary program. One of the events I already went through was the issue of the Immigration and Nationalization Service trying its pass. But the processes hadn't been thought through and made easily accessible to those individuals that wanted to use it. So it broke down just on the concept of use and the ability to easily access the program to begin with, prior to the application process.

But if we state to frequent flyers out there, if you take the members of frequent flyer groups, if you take the traveling business people, if you expand that to multi-trip individuals, the process will begin to support itself. But we've to make sure that we get it right from the beginning. Because if you lose that kind of confidence in the process you may not and see enhancements as a result of being able to utilize that, and you're not going to get anywhere.

It's absolutely paramount that what we do is focus our attention on individuals and individuals' belongings and items. Because the universe of what we're trying to do now, even under the most trying circumstances, is prone to failure, because we do not have personnel adequate for every program in every area. You really have to focus that. And so by this voluntary program, begin with those individuals who have a primary interest in the program, then expand it beyond that so that it works in the event that the primary people go.

Senator ROCKEFELLER. Well, let me follow up on that for a second with a question which I was bound to ask at some point anyway. One of the things that, it has never once in my life occurred to me that a West Virginian is any less important than somebody from New York or California. But it has often occurred to me that when it comes to programs of various sorts, that West Virginians sometimes get included and sometimes do not.

So again, we use the word "voluntary." And I can foresee a situation wherein, let's say, O'Hare and San Francisco and Denver and Louisiana, et cetera, and Miami, all of these—all of these, they have the money—which I want to talk about with you, Administrator Garvey—but they have the money to do those things or the money is made available to them because they are high-profile, high-volume airports with a lot of people going through them.

In States like West Virginia—and there are many like us—where you may have relatively few airplanes landing and therefore, much less, you know, bodies, obviously, that then to me says that voluntary is sort of like in a sense confining the good technology stuff that really cuts down on security risks to the larger airports. And says, all right, you in West Virginia, you are going to have to wait until there is proof out the American people accept it or we have the money to pay for it. Because some of these systems not only are tremendously expensive, not only to buy, but also to install. And then the people have to be ramped up to handle all of this.

So you know, as I'm interested in healthcare, I always point out that 81 percent of the counties in America have no health plans. And, you know, there is an awful lot of rural America. Those folks who did the September 11 thing entered through Maine. And so this word "voluntary," and yet how does it not conflict, if you see it that way, with the rights—the citizenship rights of small States and small airports?

Ms. GARVEY. Chip may have a different answer, but I was thinking more of voluntary on an individual basis. In other words, if I elect to be part of a program, then I can be part of it. If I'm feeling that my civil liberties are threatened or whatever, then I don't have to be. I wasn't thinking that it would be voluntary necessarily on the part of the airports. I'm just assuming that all the airports and airlines are going to want to do this. And I may be wrong on that.

Senator ROCKEFELLER. Well, I was thinking about the second as opposed to——

Ms. GARVEY. OK. And I was thinking of the individual saying, well, I am a frequent flyer and I do not mind at all. I will give you whatever information you want. I am sort of the same way that you are, that if I am selected and my bag is opened, I am pleased with that, because I do not feel threatened by that. I am delighted because I think somebody is really taking this seriously.

Senator ROCKEFELLER. A lot of people in rural areas do not fly as much.

Ms. GARVEY. Yes.

Senator ROCKEFELLER. You know, they do not go city to city or go across the world as much. They are not as comfortable with the concept of making themselves a voluntary commitment. But even that is not what I was talking about. It was a question of how you get that machinery, the detection mechanisms—as far as what you are talking about—into smaller airports, so that we are not treated in a second class sense, which to this Senator is pretty important.

Mr. BARCLAY. Let me add that the beauty of biometrics for the individual is how inexpensive they are, both for the readers and the cards. As long as we do it as an open technology and think about it in advance, the issue of passenger screening is very, very inexpensive to get done. And a lot of us who travel a lot, will wind up paying a fee to get the card at one time.

But you will always have an option in the system. The aviation system is almost exactly as you were pointing out in healthcare: 90 percent of the traffic is in the top 75 airports. But we have 500—or 450 more airports that have the security procedures in place. So there are a lot of places with very small volume. There, the advantage of streaming quickly through a very small airport is probably not as great as it is at some of these other places like Baltimore, which has 2-hour lines almost every morning these days. So the incentives may not be quite as high. It depends on how often you travel.

But we are going to give everyone in the system a different path to go if they have not bothered to get one of these biometric cards for themselves. I really think the economics of that work wonderfully for the system. And in fact, the price is coming down all the time. The more people we get in the system, the cheaper and cheaper it will get. So that part of the system is going to be set up well.

I think part of your question may go to the issue of baggage screening, where a lot of people are in favor of having 100 percent screening of all bags in the system with EDS machines. Each one is $1.2 million. There you do wind up having many multiple numbers of those machines at a number of airports when you have it set up. That is going to be a huge burden at smaller airports, and that's one we have to address as a national issue, not a local issue. So I do think there is a mix of the economics here that would work.

Senator ROCKEFELLER. Which brings us to funding. Jane, you were about to say something. You go ahead and say it.

Ms. GARVEY. Well, go ahead.

Senator ROCKEFELLER. One of the things that scares me a lot is that we are, as a society, going to decide, with what has happened after September 11 with the prospect of more of this happening, we are already now almost certainly in a budget deficit situation for next year, kind of taking us back to the 1980s.

And then if other things happen, let us say it is the power grid or let us say it is the port authority, or it is the bridges or whatever it might be, it is a tremendous demand on resources. You know, the Nation—everything that I was working on—not—and I do not mean this literally, but the focus of what I was literally working on every day in committees up until September 11 is now off to the side. And that does not mean that I am not fighting for healthcare and all kinds of other things. But they are not being paid a great deal of attention to right now, because everything is national security.

When it comes to national security, whether it is CIA or the FBI, the shortage, the enormous numbers of people needed to protect ports, railroads, airports, whatever, that money becomes a problem. Money is a problem. We are already in a recession. Now we may be in quite a deep recession. It may last for a while.

You are, Administrator Garvey, in an uncomfortable position—and I know this because everybody who works in any administration, Republican or Democratic, is that you have to toe the line, so to speak, for the Office of Management and Budget. They basically tell you what you can spend. You know a whole lot better what you need and what the American people need for security, than they do. But they have to make the numbers balance according to their objectives.

And so I want to do the best I can to coax out of you a sense of what you think this business of making America's airports and airplanes safe is probably going to cost, and then some sense of what you feel may be allocated for that. And I do not want to get you in trouble.

[Laughter.]

Ms. GARVEY. Well, it wouldn't be the first time. Actually, I think you can divide into two buckets to start with. If you think about the explosive detection equipment, as Chip said, it is about $1 million per machine. We had always been getting about $100 million a year over the last several years, and that is the pace we have been staying at.

The manufacturers are now saying that they believe they can ramp up to almost 80 a month, so that is a significantly higher number. So that number for us would be much higher, and it would certainly be much higher than the $100 million that we have gotten in the past. So if we stay at the pace that—I am just, again, going by what the manufacturers say, if you say 80—I hope your math is better than mine, you can check it—if it is $1 million a machine, 80 a month, figure out the math.

Mr. DOUBRAVA. It is over $100 million.

Ms. GARVEY. Definitely, yes. So it is quite a bit higher than we have had in the past.

The other piece is the whole area of research and technology. And I mentioned the work that this Subcommittee was doing for us in evaluating all of those wonderful technologies that may be out there. And they are looking at the airport, the perimeter of the airport, they are looking at that. They are looking at the smart card idea. They are looking at things having to do with background checks, biometrics.

The number that we have talked about internally just to get that even started is close to—million. I mean, these are very expensive ventures here. So if you think in terms of the EDS, which is a higher number; if you think in terms of research and technology. But again, I think one way to approach that might be to say, let us think of two or three airports and run a pilot program, run a model program and see how that works. And that might be a way to gain some traction, gain some understanding without taking it on full bore.

And then the third area is the whole area of the Federal Marshal program. Again, we are still working with those numbers, but we have always had a very small program. We have ramped up considerably in that one area. We have heard a lot of interest, both from Congress and the American public, wanting to have more Federal Air Marshals available. So we are certainly willing to ramp up in that area, and that would be a significantly higher number. Again, I think based on—and that is probably something that we would have to talk about in a classified situation since we do not generally review it in public. So I would say the EDS technology, the research and development, and then finally the Federal Air Marshals are the biggest areas.

Senator ROCKEFELLER. On an average pre-September 11 day, you have what, 7,000 airplanes?

Ms. GARVEY. On an average day?

Senator ROCKEFELLER. Yes.

Ms. GARVEY. Nationally—well actually at one time, at a given time, there is about 35,000 per day.

Senator ROCKEFELLER. Thirty-five thousand.

Ms. GARVEY. Yes, commercial aircraft. If you are talking about flights. Yes, flights.

Mr. BARCLAY. Commercial aircraft.

Ms. GARVEY. Yes, flights. He said 7,000, and that means at one given time.

Mr. BARCLAY. Commercial flights.

Ms. GARVEY. So during that time, that was exactly the number on the screen.

Senator ROCKEFELLER. OK. So if you would have, let us say, 30—and the figures can be bandied around—but when it started, say 32 trained sky marshals, and you have got to take that—well, not to 35,000 flights, but depending on their hours, et cetera——

Ms. GARVEY. Right. And also working——

Senator ROCKEFELLER. And that is an enormous——

Ms. GARVEY. That is a big, big number. And also working very closely with the FBI and saying where are the greatest threats, you know, and what—and that is, again, very close collaboration with the FBI. And, you know, I think someone mentioned here this morning, among panelists I know we talked about it, there is no one single solution. You have to look at it as a whole integrated package.

The fact of the matter is the airlines have done a good job in reinforcing the doors. They moved very quickly after September 11 and have reinforced, I believe at this point, all of the cockpit doors for the commercial fleet. And that is wonderful news.

So that is one part of the equation, one part of the solution. Now, Federal Air Marshals, more Federal Air Marshals, is another key point. Smart cards that Chip and you were talking about—I mean, all of those things have to be factored in as part of an integrated solution.

Senator ROCKEFELLER. Mr. Doubrava.

Mr. DOUBRAVA. Well, I think the Administrator focused on the challenge, and Senator, you know that from your experience.

Senator ROCKEFELLER. That was smoothly done, Administrator.

Mr. DOUBRAVA. But the biggest challenge, of course, is that we are not going to be able to use 100 percent application of every program, EDS, or—we are going to have to design a program based on threat, based on finding streamlined processes to get people out of the situation. I mean, clearly, we are all uncomfortable with the fact that elderly individuals are being screened robustly.

And those are the types of things that we have to find some solutions for, because as we move forward, we are not going to be able to deploy EDS—certainly not with the financial liability that we all have—at 100 percent of the airports within 2 or 3 years. And clearly, one of the things that concerns us is the technological leaps that need to take place.

We certainly would not want to spend all those resources initially on a first generation or first generation-and-a-half technology. Because clearly, we are going to get a better mousetrap; we always do. We have got to work through those processes. But we really do not want all those resources used in an immediate deployment with the current technology that we have in that particular environment. So I think that is the big challenge for all of us.

Senator ROCKEFELLER. Let me comment on that and ask a question of the three of you. I understand that, I agree that one size fits all is not particularly American. On the other hand, voluntary, which is particularly American, also says that some will be safer before others. So there is an inherit conflict.

In other words, as we are discovering what are the best technologies—and I want to get to biometrics in a moment—but what are the best ways of securing people's safety as they board, and the perimeters of airports and the whole, you know, catering service, everything—as you do things on a—not voluntary as to personal information, but you put some things out there to see if they work, and you test them and you try them. In the meantime, there are a lot of airports that are not getting the advantage of any of those, because you are probably going to be trying those at the larger airports, because you almost have to. Am I right or wrong?

Ms. GARVEY. Well, when we looked at the EDS deployment, we laid out in the last couple of weeks where we would like to see it go. We tried very hard not to use that category X. But frankly, we have got a lot of equipment out there in category X.

But we tried also to recognize that in smaller airports like Portland, for example. I mean, if it is clear that those are your points of vulnerability, then that is very exposed to terrorists and others. So we have tried to lay it out with small airports and mid-sized airports as well, both with the idea that we want to try to get it in as many different places in the system as we possibly can. So we actually tried to approach it that way.

I certainly know the Congress and your Committee has always been interested in making sure both in the AID program and other programs we have had professional air services that the needs of the smaller airports are attended to. And I hope to be able to do that.

Senator ROCKEFELLER. It is not just a question of coming from the perspective of smaller airports. It's a question of national security.

Ms. GARVEY. That is right.

Senator ROCKEFELLER. That is one thing that is always said about terrorists: They look for the weakest link, and that is why they went to Portland, Maine. And that is where this whole process of the Twin Towers, you know, began. The World Trade Center. So I do worry about that.

Now, the question I wanted to ask you was a little bit of what I asked you before, and that is: It is a little bit like in the situation that we are in, where you have international terrorism going on, horrendous television photographs, catastrophic discussions. And what happens is two things. One is that many of these are quite probably true. And second, it scares people. And I found that one of the things I do a lot of since September 11 is simply get on the radio talk shows and try to both be truthful with people about the fact that we are not talking about just one country here. We are talking about probably 60 countries that have terrorists that have angst toward this country for various reasons and are kind of planning on doing something about it, perhaps. And that that is a very serious problem.

On the other hand, you want people to be calm. So you have to both tell the truth, and in a sense say: I think we are going to be OK here in West Virginia. You cannot be absolutely sure, but you want people to be calm. Because once the American people get afraid or fearful of something, they will back off or hunker down or they will fulfill the prophecies that the terrorists want. We won't travel. We won't buy. We won't go out. We'll sit indoors and play checkers or something.

Then my question is: How do you take words like biometrics—which I think is the future, not just in aviation, but in a whole lot of other things. I think it's one of the most exciting. I can say that it is a retinal scan, which is the dark part of the middle of your eye, which is unlike—there are no two out of the 6-, 7-, 8-billion people in the world that would be the same. Or your thumbprint, or your facial thing, or the sound of your voice. Nothing—nothing—there are no two alike in the world. And you measure those.

Now, on the one hand, you are asking people to do something, if and when we come to this—which I think we will—which, in a sense, invades their history or their privacy; which perhaps puts up in their mind, well, then they now will know everything about me, whether I have diabetes or whether I, you know, got a D-minus on my French exam in the third grade or whatever.

But on the other hand, it is for their protection. It is for their protection for their safety, it is so that they feel, in fact, better about living their life, more secure about doing what they want to do. But you can only accomplish that through—and then you use the word "smart cards." And people get nervous. Well, what does a smart card do to my life? What does that mean?

So this whole question of how you integrate the positive concept of a more secure America, less vulnerable to what we went through on September 11, and then on the other hand, again, a little bit of invasion or apparent invasion of privacy. Now, we did that with credit cards. When credit cards started out, they were very unpopular. This was many years ago. And as it became more secure and people developed confidence in it, the whole credit card industry soared. In fact, it soared out of sight and probably is helping to increase our debt hourly.

But nevertheless, once people trusted it, then they saw that it was in their interest. Now, my question is: To me, biometrics is great. It is a great thing for security. Frankly, it is a great thing for West Virginia, for this university, which obviously I care about. But more importantly, it is a good thing to protect our people. And how do you work the psychology, as you throw out EDS and smart cards, all kinds of things, that you do not drive people away from what, in fact, is in their own interest. If you see it that way?

Mr. BARCLAY. I just think that the American people are real smart, and I think they are seeing it for themselves. You know, if you are Germany or Japan, you can run your country with roads and railroads because those countries are geographically small. Germany is only twice the size of Wisconsin. We have this huge country. If we do not have an airport or air traffic control system that operates efficiently, moves people quickly, moves them safely and securely, our economy is not going to move.

So you start with that explanation, and you get down to the things we need to do to provide security. You then admit that nothing is perfect. People break out of jail. We know lots about that. Human beings are clever, and we are now combating a force of special ops teams, suicide pilots who are trying to break into our system and are trying to figure out their way around any system we put in place.

So you are never going to get perfect. But I think the American public, the folks I talk to, want to see us get serious about better perimeter security, better security on the airplanes, better screening. They are not looking for perfection.

And the good news on the money side is, people are willing to pay more. All the surveys say that people are willing to pay more on the ticket. If you combine that together with the national security interest in getting some more money out of the funds that we are making available for this new world we are living in, we can get there.

These are not impossible things we are talking about doing. The technology is there and off the shelf. We can, at the same time, build public confidence by saying we are doing everything we can possible to make this as safe as it reasonably can be. You should get back about running the business of this country. Part of your job as citizens is to accept that no system is perfect, but air transportation is the safest form of transportation in the history of mankind. We move more people greater distances than anything else by far. We know we have lost public confidence since September 11. But we are going to move to get that back. We have got the systems. I think that is a message in itself.

Senator ROCKEFELLER. I want to ask each of you if you have any other comments you want to make, but I want to get in a little plug before I do that.

I don't think it is by accident that whether you are talking about *The Washington Post*, the ABC poll, or CNN poll, or whatever it is, that it is either 82 or 86 percent of the American public says that they want to see screeners in airports made—not Federal in the sense of bigger government, but made Federal in the sense they become part of the law enforcement process. They become accountable to the law enforcement process.

And the reason that they are not, in a sense, contracted out as we do, is partly because as life gets more complicated and the world increases its danger, that building into their lives the databases that involve the CIA, the FBI, the Immigration and Naturalization Service, all to protect who are the good guys and who are the bad guys so that you can separate out the bad guys and be much more secure about them, is terribly important.

And the American people are saying very directly, unless we see those screeners made a part of the law enforcement process within the Department of Justice, we are going to be slow to get back on airplanes. Is that not correct?

Mr. BARCLAY. I agree that is what the surveys have all shown a preference for.

Senator ROCKEFELLER. So that was careful.

[Laughter.]

Senator ROCKEFELLER. Chip. Jane, I will not ask you. Dick, I will ask you.

Mr. DOUBRAVA. Senator, I think that, as you know, the industry, our members firmly believe in the federalization approach. We did not push for that position on either bill, simply because we know that at the end of the day, you all will give us what we need. And the important thing is that if we move forward with this conference committee, we are anxious for you all to do your work so that we can get about doing ours. And we look forward to doing that.

Senator ROCKEFELLER. Let me just ask each of you if you have any other points that you would like to make.

Ms. GARVEY. I'd like, if I could, Mr. Chairman, to go back to your comment about the concern about the privacy. And I was thinking as you were speaking, we probably all need to do a better job of really laying that out for the American people. Because I think Chip is right. This is a smart group of people, and when it is very clear what the tradeoffs are—and people understand they need to trade off in life. And so I think we need to do a better job of that.

And I was also thinking as we look at the research and development and look over the next several weeks on the most promising technologies, particularly those that are ready to be deployed, the more we can get out there in whatever manner works, whether it is with all the Federal dollars or a combination of public and private, I think the more we can get out there to really demonstrate to people how effective these technologies can be, I think that is in all of our interests. But also speaking more directly as you did about the tradeoff and the analogy with the credit card company, which I have not followed until today, I think is a good analogy. We probably need to continue with a little bit of that message.

Senator ROCKEFELLER. OK. I will just close this panel with my thanks to you and also tell you that I am really in absolute shock that virtually 2 months after September 11, almost 2 months after September 11, that we have not passed an aviation security bill. And I think our conference starts on Wednesday. And you said Congress ends up doing the right thing. Actually, I have never heard anybody say that before.

[Laughter.]

Senator ROCKEFELLER. But we had better. We had better on this one. Thank you all very, very much.

Please come forward. The first is Jeff Planton, who is Senior Vice President of EDS, which is Electronic Data Systems out of Herndon, Virginia. Mr. John Selldorff, who is President of Automation and Control Solutions, Honeywell, and that is out of Minneapolis. And Mr. John Siedlarz, who is the incoming Chairman of the International Biometric Industry Association. So he is very important to us. And that is out of Moorestown, New Jersey. And then also Dr. Michael Yura, who is our own, who is a Ph.D and Director of the Forensic Identification Program here at West Virginia University.

Gentleman, I look forward to your testimony. Why do we not start with you, Mr. Planton.

STATEMENT OF JEFF PLANTON, SENIOR VICE PRESIDENT, FEDERAL GROUP, EDS

Mr. PLANTON. Thank you, Chairman Rockefeller. I am Jeff Planton, Senior Vice President of Electronic Data Systems. I think Administrator Garvey and I probably are going to confuse some people because I will refer to my company as EDS, not to be confused with explosive detection systems.

Senator ROCKEFELLER. I know. We all understand that explosives and EDS are quite different operations.

Mr. PLANTON. EDS appreciates this opportunity to present our views to this subcommittee on a subject of great importance to both EDS and our clients. Because EDS clients include the Federal

Aviation Administration, Immigration and Naturalization Service, domestic and international airports, and some of the largest airlines in the world, aviation security is a critical issue to us as well.

Many of the conveniences airline travelers once enjoyed have been suspended. The challenge faced by the industry going forward is to find a way to first stabilize and then continuously improve the efficiency of security processes.

The EDS approach focuses on two different areas: the passenger and the airport. For passengers, EDS recommends a process where the government or other central entity is responsible for evaluating passengers. Is an individual a threat? While airlines are responsible for identifying and authenticating passengers, is an individual who they say they are?

EDS recommends enhancing physical inspections of travelers and bags and implementing a centralized passenger evaluation system similar to the current CAPPS system, except that it is managed centrally and incorporates law enforcement watch lists.

We feel that biometric identification systems—implemented by airlines, but sanctioned by the government—could be used to speed the check-in process for frequent travelers. Having once registered with a system where foolproof identities were provided, a traveler can authenticate his or her identity in seconds at a biometric checkpoint. Viable biometric technologies today include fingerprint scanning, hand geometry, facial recognition.

While the current FAA-mandated CAPPS system is a great start, regulators, airlines, unions, and associations agree that improvements are warranted. EDS recommends a centralized passenger evaluation capability. With a centralized capability, government entities responsible for aviation security would have greater control over evaluation criteria, could quickly alter these criteria when appropriate, and instantaneously alert airlines to potential threats.

Further, this system would be a logical platform for comparison of passengers to the law enforcement watch list. Armed with this information, personnel at security checkpoints would know who to look for and could prepare for the appropriate response.

In the airport environment, key issues to be addressed around the airport security environment include: All the right personnel in the right place at the right time, all the right assets in the right place at the right time, all airport and airline employees should be issued biometrically-enabled smart cards following a rigorous background check. These smart cards could replace current identification cards, and by requiring a biometric match, any stolen or lost cards could be rendered useless immediately.

Senator ROCKEFELLER. Could you just explain again for our audience here the right definition of the word “smart card”?

Mr. PLANTON. If I can. And this is for you. This is a sample of a CAC card being given and issued to the U.S. Defense Department. On this card there is a computer chip. This card has 32 KB of memory on it. On these 32 KBs, we can a store a biometric template which, in a fingerprint—I would take my fingerprint. It would scan it. It would then read onto the chip. At that point, I have both my fingerprint template and, of course, the original finger. I carry that with me. If I put it down on a reader, it reads my fingerprint and the template so it shows that I am the same person.

On this particular card, we normally have a chip. We have got two different bar codes that can be used for information and the magnetic strip also. We have three different storage mechanisms. There are four different storage mechanisms on this sample card right now. We can start with a magnetic strip to use today's technology, and put the biometric on the chip for tomorrow's technology; and as we migrate, we go away from the magnetic strip on to the biometric chip. And I will leave this for you, sir.

Senator ROCKEFELLER. Thank you.

Mr. PLANTON. OK. As I said, also, lost or stolen cards. If I lose this card today, nobody can use it even if they have a PIN number like you do today, magnetic strips and PIN numbers. Without this finger, this card is useless, because I carry the biometric with me. Today, all I need is the magnetic strip and the PIN number, and I can get in anywhere. Pretty much like our ATM card.

In a process similar to that used for passengers and employees, airport assets and vehicles entering the airport perimeter could also be determined as "known" and "unknown." Again, this permits security resources to focus on a smaller number of unknown entities. The system involved could be tagging vehicles with radio frequency ID cards, or RFIDs, which are recognized by airport systems.

Technology will be critical to the total solution while preserving convenience, privacy, and fiscal responsibility. At the core of the security system will be information technology. This robust system will have to process data real time, will have to be linked to airports, airlines, and governments around the world. This system will require a secure, solid infrastructure.

Few of the technologies that have been mentioned today are new. EDS is issuing millions of smart cards for the U.S. Department of Defense. Israel's Ben Gurion airport utilizes biometric systems to expedite check-ins for thousands of passengers every day. Credit card systems evaluate and authorize millions of transactions using information captured at point-of-sale devices around the world.

In conclusion, secure airport terminals and tarmacs by identifying, verifying, and authenticating personnel, equipment, and shipments at critical points in the security process. Conduct rigorous background checks of employees, deploy a biometrically-enabled smart card system, employ radio frequency technology, enhance scanning capability.

Enhance passenger security by using an evaluation database and employing biometric technologies. Implement centralized evaluation and law enforcement watch list databases, deploy an opt-in biometrically-enabled smart card system to increase proportion of "known" passengers, implement alternative security processes for "unknown" passengers.

Thank you for this opportunity, and I will be glad to answer any questions you have.

[The prepared statement of Mr. Planton follows:]

PREPARED STATEMENT OF JEFF PLANTON, SENIOR VICE PRESIDENT, FEDERAL GROUP, EDS

Good morning. I am Jeff Planton, Senior Vice President with the EDS Federal Group in Herndon, Virginia. EDS appreciates the opportunity to present our views to this subcommittee on a subject of great importance to both EDS and to our customers.

After the worst terrorist attack in U.S. history, the Federal Government, airports and the airline industry are grappling with short- and long-term approaches to passenger safety. Because EDS clients include the Federal Aviation Administration (FAA), the Immigration and Naturalization Service (INS), domestic and international airports and some of the largest airlines in the world, aviation security is a critical issue for us as well.

Almost immediately after September 11th, we put together a team representing every element of the aviation industry and critical technologies, including biometrics, smart cards, information security, and complex data management. This team has identified an approach to aviation security that encompasses the passenger experience, airport environment and the underlying infrastructure.

CURRENT SITUATION

First, we should address the current situation. Many of the conveniences airline travelers once enjoyed have been suspended. Vehicle parking near terminals is severely restricted. Only ticketed passengers are allowed beyond security checkpoints. In-depth checks are being conducted before passengers are given permission to board planes. Once on the plane, passengers and baggage are again checked and accounted for.

All these restrictions are necessary to ensure security. At the same time, they add costs and constrict the flow of passengers through airports. While most Americans have accepted delays and longer lines thus far, many question how long this acceptance will last. The challenge faced by the industry going forward is to find ways to stabilize and then continuously improve the efficiency of security processes. In designing new security systems, a distinction must be drawn between security processes for handling passengers and those for airport and airline personnel.

PASSENGER EXPERIENCE

For the passenger, EDS recommends a process where the government or other central entity is responsible for evaluating passengers, while airlines are responsible for identifying and authenticating passengers.

EDS would utilize an “opt-in” process to increase the number of “known” travelers. Increasing the number of known travelers accomplishes a number of things: first, it expedites the process for the known traveler by providing dedicated queues and automated kiosks, second it improves the process for the “unknown” travelers because the known persons are removed from their queues, third it increases security for all because security resources can be focused on a smaller universe of “unknowns”. In addition to this opt-in process, EDS recommends enhancing physical detection equipment for all travelers and bags and implementing a centralized passenger evaluation system, which is similar to the current CAPPS system, except that it is managed centrally and incorporates law enforcement watch lists.

Of course, the goal of these security processes is to address these fundamental questions:

- Are they who they say they are?
- Are they a threat to security?
- Are they carrying anything illegal?

ARE PASSENGERS WHO THEY SAY THEY ARE?

Rigorous proof of identity will be an essential component of the check-in. Reviewing identity documents and manually checking security databases will be one of the most time-intensive stages of the new security process.

Because of this, we feel that biometric identity systems—implemented by airlines, but sanctioned by the government—could be used to speed the check-in process for frequent travelers. It is not inconceivable that voluntary biometric registration will become a central component of future premium flyer programs. Viable biometric technologies today include hand geometry, fingerprint scanning and facial recognition.

Having once registered with a system where full proof of identity was provided, a traveler can authenticate his or her identity in seconds at a biometric checkpoint. EDS has such a system in place today at Ben Gurion International Airport in Israel. It allows registered Israeli citizens to authenticate their identities with a magnetic card and a hand scan, shaving up to 2 hours off the wait at passport control. Currently, 15 percent of the passengers at Ben Gurion utilize this voluntary authentication system. Plus, the system can be implemented rather quickly—the initial phase of the Ben Gurion system was implemented in just 3 months.

ARE SPECIFIC INDIVIDUALS A THREAT TO SECURITY?

While the current FAA-mandated CAPPS system is a great start, regulators, airlines, unions and associations agree that improvements are warranted. EDS recommends a centralized passenger evaluation capability, likely implemented and managed by the government. With a centralized capability, government entities responsible for aviation security would have greater control over evaluation criteria, could quickly alter these criteria when appropriate and could instantaneously alert all airlines of potential threats. Further, this system would be a logical platform for the comparison of passengers to law enforcement watch lists.

This kind of system is not new. In fact, EDS is currently operating a pre-screening system similar to this for a number of U.S. airlines—processing approximately 70 million passengers annually. Given that a number of airlines already utilize this system and the FAA has rights to much of the intellectual property already, EDS feels that this version of CAPPS would be the logical foundation of a national passenger evaluation capability. For similar reasons, we also feel that such a system could be up and running quickly in perhaps 6 to 9 months depending on final requirements and funding arrangements.

Additional capabilities are also recommended. This centralized system should be integrated with airport security systems. Lists of high-risk passengers could be downloaded to airport systems; minimally each day—providing security personnel with a much-needed advantage. Armed with this information, personnel at security checkpoints would know for whom to look and could prepare the appropriate response.

ARE THEY CARRYING ANYTHING ILLEGAL?

Having evaluated passengers at the time of booking and then authenticated their identity at check-in, the next task is to ensure that they are not carrying anything illegal. Much of this task will fall to the security personnel and detection equipment at security checkpoints. Additional security would come from screening of all checked baggage and the ability to track checked baggage throughout the process.

Bar code technology and radio frequency identification devices (RFIDs, like toll tags on highways) permit the tracking of baggage through the airport. Using these devices personnel would know whether a specific bag arrived at a plane when it should have. If it did not, then they could determine where the bag was removed from the process and why. This form of electronic tracking would also facilitate the positive matching of baggage to those actually boarding an aircraft. If a person's bag was loaded, but the passenger did not board, then this technology would allow personnel to quickly locate and remove the unattended checked baggage.

AIRPORT ENVIRONMENT

Key issues to be addressed around the airport security environment include:

- Are the right personnel in the right places at the right time?
- Are the right assets in the right place at the right time?

ARE THE RIGHT PEOPLE IN THE RIGHT PLACES AT THE RIGHT TIME?

Similar biometric systems that are used for known passengers could be used for airport and airlines employees as well. Just as known passengers "enroll" in the system, all airport and airline employees would be issued biometrically-enabled smart cards following a rigorous background check. These smart cards could replace current identification cards, which can be stolen and/or easily forged. Requiring a biometric match would render any stolen or lost card useless and smart cards are all but impossible to forge.

Using smart card technology, specific personnel could be permitted access to specific locations at specific times. For example, an aircrew might only be allowed access to a particular gate for a specific flight. This is far different from universal access processes currently used at most airports, which allow anyone with the correct code access to secure terminal areas or tarmacs at any time. RFID (or radio frequency identification) technologies could also be imbedded into smart cards and notify authorities if an unauthorized individual is attempting to enter a restricted area.

ARE THE RIGHT ASSETS IN THE RIGHT PLACE AT THE RIGHT TIME?

In a process similar to that used for passengers and employees, airport assets and vehicles entering the airport perimeter could be determined as "known" or "unknown". Again, this permits security resources to focus on a smaller number of unknown entities.

EDS recommends the deployment of systems such as those currently used on the U.S. borders with Canada and Mexico. These systems involve tagging vehicles with RFID devices similar to toll tags, which are recognized by airport systems. It is even possible to tie a specific employee to a specific vehicle, providing greater assurance that a given vehicle is where it is supposed to be.

To improve security around items such as catering trucks, it would be possible to utilize certain supply chain technologies that track inventory throughout a production process. Particular shipments are inspected and sealed at their point of origin (perhaps a catering kitchen). Tracking technologies could verify that a shipment remained sealed throughout the transport process and would prompt security personnel to respond in the event that a seal was broken or even if a shipment strayed from an assigned path.

AT THE CORE OF SECURITY SYSTEMS: INFORMATION TECHNOLOGY

A great deal of attention and energy has been devoted to physical security processes. This is necessary and very important, and will continue to be a key component of the security screening process. However, technology will be critical to a total solution that enhances security while preserving convenience, privacy and fiscal responsibility. Such an information system will have to process data real-time and will have to be linked to airports, airlines and governments around the world. Robust systems permitting central data management with greatly distributed data collection are required. This system will require a solid infrastructure and no possibility of downtime. And without question, access to it and to the information it contains must be secure.

While the integrated system described above is not currently in place, none of the individual technologies described are new. EDS is issuing millions of biometrically enabled smart cards for the U.S. Department of Defense. EDS pre-screens millions of passengers using its client-server system every year. Israel's Ben Gurion Airport utilizes a biometric system to expedite check-in for thousands of passengers every day. Credit card systems evaluate and authorize millions of transactions using information captured at point of sale devices around the world. And, supply chain systems track the production of millions of products in the U.S. and abroad.

Beyond the individual solutions, the scale and scope of this system would not be unprecedented, either. While integration of such disparate databases and complex technologies on a global scale might be new to airports and the airline industry, global service providers like EDS already have extensive experience creating and running comparable systems in other industries.

CONCLUSION

The challenge is to stabilize and then improve the efficiency of the aviation security processes. It is important to address both security processes for handling passengers and those for airport and airline personnel.

Secure airport terminals and tarmacs by identifying, verifying and authenticating personnel, equipment and shipments at critical points in the security process.

- Conduct rigorous background checks of employees.
- Deploy a biometrically enabled smart card system.
- Employ radio frequency (RF) technology.
- Install scanning equipment.

Enhance passenger security by implementing an evaluation database, emphasizing biometric technologies.

- Implement centralized evaluation and law enforcement watch list database.
- Deploy an "opt-in" biometrically enabled smart card system to increase proportion of "known" passengers.
- Implement alternative processes for "unknown" passengers.

Thank you for this opportunity to present this testimony. I am happy to answer any questions you might have.

Senator ROCKEFELLER. Thank you very much.

Mr. Selldorff.

STATEMENT OF JOHN SELLDORFF, PRESIDENT, HONEYWELL AUTOMATION AND CONTROL SOLUTIONS

Mr. SELLDORFF. Thank you, Mr. Chairman, for the opportunity to testify before you today on the important issue of airport security technologies. I would like to thank you also for your past leadership on critical aviation issues, and we look forward to working with you in the future as we address the problems that lie ahead.

Honeywell is a diversified global technology and manufacturing leader. We have an unusually broad perspective on airport and aviation safety. Among our core businesses, we are a leading international provider of aircraft safety communications, and guidance control systems and products; including systems to alert flight crew and ground authorities of an airborne emergency, collision avoidance, and improved flight data and cockpit voice recorders. We also manufacture Spectra, the lightest weight ballistic material made, which can be used to harden and make bulletproof cockpit doors.

On the ground, we are a global expert in control technologies for buildings, homes, and industry. Honeywell has designed and installed control systems providing security, life safety, energy, and building control management in more than 200 airports, from San Francisco and Miami to Moscow and Hong Kong.

Today I will talk briefly about the current U.S. approach to airport security and threat-detection systems; I will outline safety-enhancement opportunities incorporating existing technologies; and I will discuss what needs to change to ensure that airport workers, passengers, and airline crews can move through our Nation's airports with a minimum of risk.

Every modern airport relies on multiple control systems, from video surveillance and access control systems to equipment that manages lighting, fire detection and protection, and heating, ventilation, and air conditioning. In most U.S. airports, these systems run independently of each other and are managed by different departments. The purchasing decisions for these stand-alone systems also tend to be made separately based on two primary factors: basic functionality and lowest initial price.

The result of the current approach is that the typical domestic airport's key operational systems don't communicate with each other. There is little or no integration among the various security and safety-related systems in an airport, let alone with the building's critical operational systems.

These types of airport systems have been adequate in the past. But in this new environment, we need solutions that provide multiple layers of protection, incorporating threat-detection and response capabilities from the time someone approaches the facility and passes through security, to when they approach the aircraft and other secured areas. Airports need early warning tools to avert problems at the earliest possible opportunity, or lacking that, to respond quickly to contain damage and risk.

The answer does not lie in individual technologies; it resides in the integration of current and emerging systems. It is possible today to tie together virtually every aspect of an airport's operation into a single, powerful management solution, in effect, casting a tightly woven, protective net over the airport and its occupants. Such systems not only integrate video surveillance, access control, fire, emergency evacuation, and other types of safety-related systems, they also link critical operational systems that control such functions as lighting, heating, ventilation, and air conditioning. The systems can be programmed to automatically take certain actions in the event of an incident, across a variety of functions.

Say that an unauthorized person enters an area containing critical building equipment. The access control system sounds an alarm on the staff's workstation and indicates where the breach has occurred. On the same screen, the video surveillance system displays live footage of the area so security staff can determine an appropriate response. At the same time, other types of building management systems would be alerted and automatically respond based on preprogrammed instructions. Depending on the situation, perhaps the ventilation units would shut down and doors in the area automatically lock.

Integrated solutions also can provide data from human resources such as employee photo and work schedules as well as other databases for known criminals. The result is to turn raw information into intelligence that the facility operators and its systems can act upon. For instance, based on employees' work schedules, the access control system can limit entry to only those employees who are scheduled to work or travel on that plane.

As biometric technologies such as facial recognition become more prevalent, they will be able to communicate with airport personnel databases to prevent the use of stolen access cards. In an integrated system, the access control system will be able to compare the card code to the face or fingerprint stored in the employee's file and deny access to anyone other than that particular worker.

An integrated system that included access to FBI and other law enforcement databases would provide an additional and much-needed security enhancement. Armed with the images and backgrounds of known terrorists, an airport's security system could proactively identify potential threats and facilitate a response before any damage is inflicted.

Integrated systems are not just a possibility; they are a reality at a growing number of airports outside the United States. Currently, 70 percent of the airport systems that Honeywell has installed are outside the United States, in facilities that seek to capitalize on the benefits that integration provides.

There are several reasons why international airports are adopting integration technologies. One, of course, is more experience with terrorists. In fact, the European Union encourages the use of integrated security systems in its member country airports. Elsewhere, the Sydney, Australia, Kingsford Smith Airport installed a 100-camera digital video surveillance system that integrates to a security management system in preparation for the 2000 Olympic Games, while also setting the groundwork for future passenger growth.

Airports outside the United States are utilizing integrated systems for broader, long-term business reasons. Such systems increase staff productivity and effectiveness. Through their ease of use and centralized, comprehensive control capabilities, they reduce energy costs by permitting automatic, timed control of equipment. At the Munich Airport, for example, a comprehensive control solution allows operators to activate runway lights, heating, ventilation, and air conditioning in specific gate areas, and even baggage carousels, based on flight schedules.

Airports outside the United States generally view their building systems as a long-term investment. They tend to select systems based not on initial price, but on the systems' ability to lower the facility's life-cycle costs. And they look beyond current functionality, seeking flexible systems that will accommodate new technologies and support business changes.

The current situation presents both a short-term challenge and a long-term opportunity. It is critical that we place the best technologies and procedures throughout our Nation's airports. Integrated solutions should be deployed wherever possible.

The industry will continue to come forward with new technologies and ideas to enhance airport security and avert emergencies. But the Federal Government must play a leadership role in creating and implementing this security plan. Standards must be developed and mandated that provide a security framework that is adaptive based on a given airport's usage.

The Federal Government must lead the effort to create these national standards so that safety and risk-mitigation capabilities are consistent from airport to airport. Equally important, it needs to implement policies that will streamline the certification, regulatory, and procurement processes so solutions can be fielded quickly.

The FAA has projected that in the next 20 years, domestic passenger enplanements will double, and commercial aircraft operations will increase by 47 percent. Clearly, the time to put more stringent airport security measures in place is now. We must take steps to rebuild the confidence of the American flying public and provide them with airports that are truly safe and secure.

Thank you for the opportunity to appear before this Subcommittee.

[The prepared statement of Mr. Selldorff follows:]

Prepared Statement of John Selldorff, President, Honeywell Automation and Control Solutions

Thank you, Mr. Chairman for the opportunity to testify before you today on the important issue of airport security technologies. I would like to thank you also for your past leadership on critical aviation issues that affect every citizen in this country and we look forward to working with you and other members of the Committee as we address the problems that lay ahead.

By way of background, Honeywell is a diversified global technology and manufacturing leader. We have an unusually broad perspective on airport and aviation safety. Among our core businesses, we are a leading international provider of aircraft safety, communications and guidance control systems and products—including systems to alert flight crew and ground authorities of an airborne emergency, collision avoidance and improved flight data and cockpit voice recorders. We also manufacture Spectra, the lightest weight ballistic material made, which can be used to harden and make bulletproof cockpit doors.

On the ground, we're a global expert in control technologies for buildings, homes and industry. Honeywell has designed and installed control systems providing security, life safety, energy and building control management in more than 200 airports, from San Francisco and Miami to Moscow and Hong Kong.

Today, I will talk briefly about the current U.S. approach to airport security and threat detection systems. I will outline safety-enhancement opportunities incorporating existing technologies. And I'll discuss what needs to change to ensure that airport workers, passengers and airline crews can move through our nation's airports with a minimum of risk.

AIRPORT SECURITY SYSTEMS TODAY

The events that began unfolding Sept. 11 have changed the rules. Across every aspect of American society, the policies, procedures and systems that once seemed adequate now are called into question—and often found in need of change. That is true of how U.S. airport security systems are planned and implemented as well.

Every modern airport relies on multiple control systems, from video surveillance and access control systems to equipment that manages lighting, fire detection and protection and heating, ventilation and air conditioning. In most U.S. airports, these systems run independently of each other and are managed by different departments. The purchasing decision for these stand-alone systems also tend to be made separately, based on two primary factors: functionality (e.g., how well does this system provide video surveillance) and lowest initial price.

The result of the current approach is that the typical domestic airport's key operational systems don't communicate with each other. There is little or no integration among the various security and safety-related systems in an airport, let alone with the building's critical operational systems. If an incident occurs, airport management cannot obtain a timely, single view of what is happening. Instead, they need to go into multiple systems. In other words, once the access control system indicates a security breach, the operator must enter a separate closed-circuit-TV surveillance system to view the intruder and what he or she is doing. Responding to the incident often requires multiple steps as well.

These types of airport systems have been adequate in the past. But in this new environment, we need solutions that provide multiple layers of protection, incorporating threat-detection and response capabilities from the time someone approaches the facility and passes through security, to when they approach the aircraft and other secured areas. Airports need early warning tools to avert problems at the earliest possible opportunity—or, lacking that, to respond quickly to contain damage and risk.

INTEGRATED SYSTEMS THAT HELP PREVENT AND CONTAIN INCIDENTS

Much attention has been given to such security technologies as biometrics and facial recognition systems. Yet these need to be part of a comprehensive solution needed to keep our airports safe.

The answer doesn't lie in individual technologies; it resides in the integration of current and emerging systems. It is possible today to tie together virtually every aspect of an airport's operation into a single, powerful management solution, in effect casting a tightly woven, protective net over the airport and its occupants. Such systems not only integrate video surveillance, access control, fire, emergency evacuation and other types of safety-related systems; they also link critical operational systems that control such functions as lighting, heating, ventilation and air conditioning.

In this integrated management solution, the airport's systems communicate and work together. The systems can be programmed to automatically take certain actions in the event of an incident, across a variety of functions. The solution also provides management with a single centralized view of the building's operations, enhancing intelligence during an incident while strengthening overall facility management day-to-day.

Integrating an airport's systems provides a higher and more effective level of operational control, less opportunity for human error, greater responsiveness in the event of a problem and less public exposure to risks. Let me give you an example of what I mean.

Say that an unauthorized person enters an area containing critical building equipment. The access control system sounds an alarm on the staff's workstation, and indicates where the breach has occurred. On the same screen, the video surveillance system displays live footage of the area, so security staff can determine an appropriate response. At the same time, other types of building management systems would be alerted and automatically respond, based on pre-programmed instructions. Depending on the situation, perhaps the ventilation unit shuts down, and doors in the area automatically lock.

USING DATABASE INFORMATION FOR BETTER DECISIONS

Integrated solutions also can incorporate data from human resources such as an employee's photo and work schedule as well as other databases for known criminals. The result is to turn raw information into intelligence that the facility's operators and its systems can act upon. For instance, based on employees' work schedules, the access control systems can limit entry to only those employees who are scheduled to work or travel on that plane.

As biometric technologies such as facial recognition become more prevalent, they will be able to communicate with airport personnel databases to prevent the use of a stolen access card. In an integrated system, the access control system will be able to compare the card code with the face or fingerprint stored in the employee's file, and deny access to anyone other than that particular worker.

An integrated system that included access to FBI and other law enforcement databases would provide an additional and much-needed security enhancement. Armed with the images and backgrounds of known terrorists, an airport's security system could proactively identify potential threats and facilitate a response before any damage is inflicted.

INTEGRATED SYSTEMS CURRENTLY IN USE OUTSIDE THE UNITED STATES

Integrated systems aren't just a possibility. They are a reality at a growing number of airports outside the United States. Currently 70 percent of the airport systems that Honeywell has installed are outside the United States, in facilities that seek to capitalize on the benefits that integration provides.

There are several reasons why international airports are adopting integration technologies. One, of course, is more experience with terrorists. In fact, the European Union encourages the use of integrated security systems in its member countries' airports. Elsewhere, the Sydney, Australia, Kingsford Smith Airport installed a 100-camera digital video surveillance system that integrates to a security management system in preparation for the 2000 Olympic Games, while also setting the groundwork for future passenger growth.

In addition, airports outside the United States are utilizing integrated systems for broader, long-term business reasons. Such systems increase staff productivity and effectiveness, through their ease of use and centralized, comprehensive control capabilities. They reduce energy costs by permitting automatic, timed control of equipment. At the Munich Airport, for example, a comprehensive control solution allows operators to activate runway lights, heating, ventilation and air conditioning in specific gate areas and even baggage carousels, based on flight schedules.

And finally, such systems help deliver operational efficiencies. With key systems and databases linked together, airport management gets a full, real-time view of all operations. Operators have the information they need to improve the building's performance and the power to make facility-wide adjustments based on changing needs or single events.

These are the types of long-term benefits that airports can and should seek to capture. Airports outside the United States generally view their building systems as a long-term investment. They tend to select systems based not on initial price, but on the systems' ability to lower the facility's lifecycle costs. And they look beyond current functionality, seeking flexible systems that will accommodate new technologies and support business changes.

A FLIGHT PLAN FOR U.S. AIRPORT SECURITY

The current situation presents both a short-term challenge and a long-term opportunity. We need to establish a flight plan, if you will, to improve the safety and effectiveness of U.S. airports. And we need to do it now.

Honeywell agrees with the recommendations outlined in the U.S. Department of Transportation's Airport Security Challenge Report. Those recommendations must be implemented as soon as practicable. In particular, we strongly support the establishment of an Aviation Security Technology Consortium of public and private sector individuals to identify, sponsor and test new security-related technologies at our Nation's airports. Honeywell would be honored to participate in such an association.

It is critical that we place the best technologies and procedures throughout our nation's airports. Integrated solutions should be deployed whenever possible. For maximum return on investment, they should improve operations as well as safety. They should be built on non-proprietary languages and certifications to avoid dependence on specific technologies or manufacturers. And they must be designed to be future-proof.

The industry will continue to come forward with new technologies and ideas to enhance airport security and avert emergencies. But the Federal Government must play a leadership role in creating and implementing this airport security flight plan. Standards must be developed and mandated that provide a security framework that is adaptive based on a given airport's usage (international versus domestic versus private). Standards that take into account the technologies, the systems and appropriate databases needed to create a comprehensive, cohesive, holistic airport security management plan.

The Federal Government must lead the effort to create these national standards, so that safety and risk-mitigation capabilities are consistent from airport to airport. Equally important, it needs to implement policies that will streamline the certification, regulatory and procurement processes, so solutions can be fielded quickly.

The FAA has projected that in the next 20 years, domestic passenger enplanements will double, and commercial aircraft operations will increase by 47 percent. Clearly, the time to put more stringent airport security measures in place is now. We must take steps to rebuild the confidence of the American flying public, and provide them with airports that are truly safe and secure.

Thank you for the opportunity to appear before this subcommittee.

Senator ROCKEFELLER. Thank you very much.

I have just got to interject one thought here. Initially, you said that some international airports are using it, that ought to, should it not, be of some comfort to the American people? In other words, those that have dealt with these kinds of problems before on a relatively routine basis, as opposed to we in this country who have not, have opted toward much tougher technological and, ultimately, much safer solutions. That should be some comfort, I would think, to the American people.

Yes, sir.

STATEMENT OF JOHN E. SIEDLARZ, VICE CHAIRMAN OF THE BOARD, INTERNATIONAL BIOMETRIC INDUSTRIAL ASSOCIATION

Mr. SIEDLARZ. Mr. Chairman, I thank you for the privilege of appearing before the Subcommittee today for the biometrics industry. I sat with rising excitement during the initial committee discussion because of both the increasing recognition for the role of biometrics and the acceptance of its capabilities and what it might provide. And of course, your known support for the industry and the work that is going on here in West Virginia, we appreciate that very much.

Some 3 years ago, four small businesses engaged in biometrics with different kinds of technologies put aside their aggressive competitiveness for a short period to form the Association. The Association has grown today to over 20 companies, and it is growing even more as we speak. And one of the reasons we did that at the time is because even though the biometric industry has been emerging for some 25 years, dating back to the late 1960s and early 1970s, the truth of the matter is that we recognize that the need for public advocacy and public education is still true today, for many of the points that you raised about it in your discussions of the early industry still apply.

It's good to note that of the four companies that were represented at the time, brought together with the foresight of Mr. Bill Wilson from California, who headed then-RSI, Incorporated, who is with us today and who deals with hand recognition technology, joined me and my company with Iris Recognition Technology, then IriScan, and now Iridian Technology, and Identix, with the fingerprint, represented today by Mr. David Shipman. And also Visionics, facial recognition, represented today by Frances Zelazny.

So those four companies, as I said, put aside the differences that we saw we had, to emphasize the fact of the similarities that we had to bring to the public and the Nation what we thought was important, and has become even more important since 9/11.

I have separately submitted a written statement for the record, a letter which describes the IBIA position regarding the role of biometrics in a comprehensive aviation security program. It offers specific recommendations for consideration by the Subcommittee and the Congress in the ongoing work to improve the security of our air transportation system. With your permission, I would like to offer some brief comments that amplify our scope and hopefully provide additional perspective on the use of biometrics in commercial aviation operations under the threat of international terrorism.

Terrorism, and indeed all criminal activity, thrives in an environment of ambiguity and false identity. Rights that we have come to expect as Americans, such as privacy and freedom to travel, are exploited and corrupted by those who would have us live in fear, with the intent to cripple our society and our economy. Without surrendering those rights—and I would like to return to that issue—we need to fight back effectively and deny them the opportunity for such exploitation.

In my first 20-year career as an Air Force officer, I was deeply involved in the design and implementation of security programs for military aviation. We believed then that a world of difference separated our needs from that of commercial aviation. I believe that that world of difference was dramatically narrowed on September 11.

There are fundamental similarities in the goals of aviation security in each sector, as well as unique characteristics. We can learn from those similarities, which include the following: One, protect the air crews, aircraft, and servicing personnel by effectively denying access to the tarmac to those who are not authorized to be there. Reliable real time identification is required to achieve that goal.

Two, protect the terminal and the facilities that service and control the air operations, and the public that needs access by the effective surveillance in key areas and screening and controlled access in critical areas. Identification and authentication, properly integrated, is required to achieve that goal.

Three, protect the traveler by positive controls of baggage and boarding process, and positive identification of those who use the transportation system, especially those who cross our borders. Biometric technology in its varied forms is capable today, as it was not many years ago when I dealt with it first, of providing both a surveillance and positive identification component of these necessary security program elements. It is necessary to match the technology to the application, because no single technology can do it all. I return to that. One size does not fit all.

To those who say that the technology is not free of error in all applications, I would say, if not this, what? All current non-biometric designs and methods to solve the identification need do not work, incapable of any acceptable or realistic percentage of success. And they are measured against technology that now can demonstrate performance up to the 99 percent level in proper integrations.

To those who say we cannot identify a terrorist until he is enrolled in a biometric database, I say, if not now, when?

Some biometrics can make effective use of existing databases, and all of those who enter the United States should begin to enroll right now. To those who say it will take time to build a database for full effectiveness in antiterror operations, I say that the database controlling access to the tarmac, for the protection of air crews, aircraft, servicing personnel, facilities and the public can be accomplished very quickly.

Finally, to those who say that privacy, civil liberties, and convenience must all be sacrificed to achieve these goals, I say that you are wrong, and that your good intentions should be directed to working with the industry to minimize the impact and achieve reasonable results. If we cannot use effective technology that is capable of protecting our identity while removing the cloak of the imposter, then we will be held hostage as a society crippled by fear, intimidation, and ignorance. That is a society in which privacy and civil liberty and freedom of movement become meaningless concepts.

Privacy and biometrics, I would add, Mr. Chairman, are not incompatible. I have carried a military identification card for some 43 years. Aside from being proud of that, adding on a biometric template, whether that be iris or fingerprint or facial or whatever that happens to be, simply makes that card secure. It does not really add a single degree of personal data to the card. But it does say for once—and for the first time, I should say, in 42 years—that is my card.

And the same way for your card that you showed earlier to the panel with regards to a guarantee that that card belongs to you and not to anyone else. That is fundamentally the difference. It is possible to separate personal identities from biometric information so cleanly, so effectively that a reasonable compromise certainly can be worked to make sure that those rights and those privileges are still preserved.

Senator ROCKEFELLER. Can I just interject something here? A lot of people when they hear about cards and the availability of data through cards, automatically think, well, you know, whatever health problems or my D-minus in the third grade in French or whatever are going to become public knowledge. In other words, the whole concept of telemarketing as opposed to what it is that you are doing this for. Could you help us understand that telemarketing is not what we are talking about here?

Mr. SIEDLARZ. As a matter of fact, Mr. Chairman, I think sometimes the aggravation we see over this privacy issue is that we see a little more concentration on protecting our privacy against telemarketing than we would in some of the areas that we are concerned with here. But in any event, I hope I can.

Let us think of it this way: We like to say sometimes in the industry that biometrics can make a dumb card smart and a smart card good. I think it is important to understand that if you have a smart card without biometrics, you have a card that can contain data. That data could be medical information. It could be political information. It could be financial information. It could be almost any other information.

If someone gets access to that card and has the methodology to extract that data, because there is no protection from them to do so, then yes, that may be a serious threat to the privacy of the information that is stored on that card.

If the card is nothing more, like most credit cards, than the vehicle to get to a central database which has the extensive information, then that is something of another matter. Those might be referred to as dumb cards, but they still, in fact, make the translation from how you are effectively using it in a transaction to where that information is really stored. But that is essentially the difference between the two cards, if I properly understood your question.

Senator ROCKEFELLER. And in any event, we are facing precisely the same set of problems as we deal with the Internet.

Mr. SIEDLARZ. Absolutely. Absolutely. And biometrics, as you know, have a major role there in terms of protection of identity and the security of transactions; knowing who, in fact, is initiating the transaction and who is receiving it, with appropriate encryption and other protective devices in between to protect the data.

Senator ROCKEFELLER. Thank you.

Mr. SIEDLARZ. Yes, sir. Well, that concludes my testimony.

[The prepared statement of Mr. Siedlarz follows:]

PREPARED STATEMENT OF JOHN E. SIEDLARZ, VICE CHAIRMAN OF THE BOARD, INTERNATIONAL BIOMETRIC INDUSTRY ASSOCIATION

Mr. Chairman and Members of the Subcommittee, thank you for inviting the biometric industry to offer its views at this important proceeding. My name is John E. Siedlarz. I am the founder of IriScan, now Iridian Technologies. I am also Vice Chairman of the Board of Directors of the International Biometric Industry Association (IBIA), and I represent IBIA here today. IBIA is based in Washington, DC and advocates the collective interests of leading manufacturers and developers of biometric technology.

My company was one of the four charter members of IBIA. All three other charter members are represented here today. They include Visionics, whose Chief Executive is Joseph Atick, represented today by Frances Zelazny; Identix, represented today by David Chapman; and Recognition Systems, represented today by Martin Huddert, Chief Executive Officer, and Bill Wilson, Managing Director. Bill is also Chairman of the Board of IBIA.

THREATS TO AVIATION

Terrorism, and indeed all criminal activity, thrives in an atmosphere of anonymity and false identity. Freedom to travel, a treasured benefit in our democratic society, is exploited and corrupted by those who would threaten all movement, all travel, creating the image of imminent danger in the attempt to impose fear on our population and cripple the economy. We need to deny them that opportunity without sacrificing our rights of travel in a free society.

Piecemeal, hurried, and reactive measures for aviation security may provide a temporary solution to a specific problem, but a well designed and comprehensive security program is necessary to deter and detect threats over the long-term fight against international terrorism. No program will be complete without an effective component for identification of all participants in the travel process, as well as an efficient tool to deny access and travel to those who threaten that process. Biometric technology can be that effective component.

BIOMETRIC TECHNOLOGY

Biometrics are defined as the automatic identification or identity verification of an individual based on physiological or behavioral characteristics. The authentication of identity is accomplished by using computer technology in a non-invasive way to match patterns of live individuals in real time against enrolled records. Examples of the patterns used for biometric identification include those made from the image of a fingerprint, the geometry of the hand, and unique patterns in a person's iris, voice, signature, or face. It is important to note that most biometric applications do not store the actual image of the feature being measured. Instead, biometrics secure systems and protect an individual's identity by converting the measurement into an encrypted file. This biometric record cannot be reverse engineered to determine a person's age, sex, race or other sensitive information. Likewise, it cannot be used to steal someone's identity.

With these characteristics, biometrics are the only technologies that can offer an effective response to the need for authentication as a primary component of increased security without sacrificing convenience. The U.S. Government has been an early adopter of biometrics, first using the devices to control access to highly sensitive facilities such as nuclear power plants and weapons facilities. Now, use of biometrics is expanding to protect networks against intrusion by hackers, to secure records from identity theft, to ensure benefits are disbursed to the lawful recipient, and to protect borders.

In parallel with its efforts to work with the Government to develop and refine self-contained applications for biometric technology, the industry has worked diligently to establish the standards needed for true interoperability. In cooperation with the National Institute of Standards and Technology, IBIA has created a registry that enables any biometric device to be recognized on a network. The industry and government also have worked together to publish rules on how biometrics are to be integrated into computer operating systems. This is an exceptionally important advancement for several reasons:

- It allows multiple biometrics to be accommodated;
- It allows the quick adoption of new biometric technologies as they are developed in the future;
- It permits the rapid exchange of information for record checks; and
- It enables users to voluntarily share biometric information that has been acquired by other sources, such as employers, airlines, and government agencies.

On a broader scale, the industry and its research and academic partners, including West Virginia University, are working on new initiatives to marshal the resources of the biometric community for the common good. Such initiatives would focus on the critical need for an identification component in the security programs that protect the national infrastructure, including the aviation industry.

BIOMETRICS AND AVIATION SECURITY

In the air transport environment biometric solutions are used to handle such diverse tasks as automating immigration clearance processes for arriving international passengers, and preventing unauthorized people from gaining access to sensitive areas of the airport. This real-world experience has proven that biometric technologies perform reliably, and that they can measurably improve the security of U.S. airports, help make air travel as safe as possible, and deter criminals from entering the U.S. via the commercial air transport system. There are three specific applications of biometric technology that can be used to achieve a new level of security. They are:

- Controlling employee and air crew access;
- Identifying suspected terrorists and other people whose presence signals a danger to the airport premises and the traveling public; and
- Simplifying the often cumbersome process of identifying legitimate travelers.

CONTROLLING ACCESS

Federal Aviation Regulations require airports to adopt physical access controls that prevent unauthorized parties from getting through airside security or gaining access to aircraft ramp areas, baggage rooms, and other sensitive airport facilities. Some controls are staffed, such as entry gates and terminal security checkpoints. Others—including most doorways in an airport—are accessed by having the employee swipe a card through a reader and enter a personal identification number (PIN). Aviation security experts have identified this process as a major vulnerability, since badges and PINs can be stolen or loaned to an imposter.

Leading airports have recognized this situation and replaced the PIN with biometrics. San Francisco and Chicago O'Hare now use hand geometry and finger imaging, respectively, to control employee access through unstaffed doorways. Unless the employee has been enrolled in the system, he or she cannot operate the doorway. More importantly, enrolled employees—some 55,000 workers in the system at O'Hare—cannot pass on this identity to someone else, and the biometric information cannot be borrowed and used by an unauthorized party. Advanced versions of biometric access control systems combine the technology with sophisticated software that can limit users to certain doorways at certain times, and can track who accesses which door at what time.

Another kind of biometric access control system is being used to screen USAirways crewmembers as they pass through airside security checkpoints in Charlotte. In this trial, over 6,000 enrolled airline employees clear controls through a fully automated process that uses iris recognition technology.

SECURING THE TERMINAL

Preventing terrorists from compromising airport access control systems is an important step that can significantly reduce our vulnerability to attacks, especially those that are designed to take over commercial aircraft and use them as tools for destruction. Another application of biometric technology can help to reduce a second threat—that which is caused by a security risk who is posing as a regular traveler.

Law enforcement and intelligence authorities may have the name and photograph of a suspected terrorist, but they do not have an efficient way of linking the person's identity to someone who is traveling under a false name. Face recognition technology, because of its unique surveillance capability can help reduce this threat. Used alone, or in conjunction with other highly accurate authenticators, it can be a valuable tool for preliminary identification of a threat. This biometric operates in conjunction with the closed circuit video camera systems that are installed at most airports. Images of travelers are acquired by the cameras and converted into a template that is an encrypted digital representation of the image. The template can then be used to instantly compare the "live" images of travelers against an index of suspects.

This technology works under some very challenging circumstances. Face recognition systems that have been tested on city streets have produced a significant drop in crime rates through detection and deterrence. In an airport environment, having this capability could help overcome the challenge faced by law enforcement authorities of knowing where terrorists will be, and of recognizing them when they are there.

IDENTIFYING TRAVELERS

The new security requirements have made it less convenient for most travelers. Airlines are advising customers to show up 2 to 3 hours in advance of flight time to contend with significantly longer queues—particularly those for airside security checks—even though the system is running well below pre-September 11 capacities. Under these conditions, customers are unlikely to return soon unless something is done to alleviate the bottlenecks in the system.

Biometric technology offers several opportunities to do exactly that. The clearest demonstration of this capability is in border control, where biometrics have been used in this sensitive national security application to routinely admit pre-registered passengers. The U.S. has had such a system in place since 1993, as have Canada, Israel, the Netherlands, and Singapore. The question is how we take these low volume trials and efficiently convert the lessons learned into a comprehensive system that both tightens security and improves service levels. Fortunately, the tools are in place to accomplish this goal: the technologies are reliable, standards are in place, and we are convinced there are ways to accomplish this objective at reasonable cost without having to resort to a national identity card.

There are a number of air terminal processes that can be both automated and made more secure by turning to biometrics. Under the new procedures adopted after September 11, passengers are now required to produce a photo identification card at check-in, security clearance, and again at the gate. By enrolling passengers in a biometric-enabled system, all three processes can be significantly streamlined: instead of waiting in line at check-in, passengers can use self-service kiosks to obtain tickets and boarding passes; at security checkpoints and boarding gates where biometric readers are installed, a passenger's identity can be verified without having to again show a boarding pass, ticket, or ID card. This is not just more convenient for the traveler; it also reduces the chance of human error in security screening tasks, and provides a real opportunity to be more efficient in how queues are managed for everyone using the system.

RECOMMENDATIONS

Biometric technologies can be a critical component of an air transport system that offers both improved security and better service under the exceptionally difficult conditions the industry faces today. There are a number of steps that Congress can take to ensure that this vision becomes a reality.

EMPLOYEE IDENTIFICATION AND TERMINAL SECURITY

The Federal Aviation Regulations at 14 C.F.R. Section 107.14 call for an employee access control system that ". . . shall provide a means to differentiate between persons authorized to have access to only a particular portion of the secured areas and persons authorized to have access only to other portions or to the entire secured area." While this section calls for the means to "differentiate between persons," it do not mandate the explicit use of biometric technologies for positive identification of workers who have access to sensitive areas of the airport. As noted above, Chicago O'Hare and San Francisco have been aggressive in interpreting the intent of the regulation and have installed biometric devices to make certain that only authorized individuals could pass through secure portals. These systems measurably improve physical security and simplify the administration of security systems. IBIA recommends that Congress amend Title 49, Subtitle VII of the United States Code to require positive biometric identification of all people who are given access to secure airport areas.

Security checkpoint processing for aircrews can also be improved through the adoption of biometric verification technologies. Earlier efforts to standardize crew ID systems throughout the U.S. air transport system have not come to fruition, largely due to questions about harmonizing the format and features of aircrew identification documents. With advances in network-based biometric systems, airports and airlines are now able to simplify identification without having to standardize or reissue ID cards. We therefore highly recommend that gaps in security that could be caused by aircrew imposters be eliminated by mandating the use of biometrics for positive identification at airport gates, airside security checkpoints, and other vulnerable locations.

Intercepting potential threats at an airport is a daunting task. Using biometrics in employee- and aircrew-identification systems can reduce the scope of the problem, but many vulnerabilities remain. Face recognition technology can help law enforcement officers overcome this challenge by giving them a tool that can help locate the 1 person in 10,000 who may pose a risk to facilities, aircraft and travelers. We urge Congress and the Federal Aviation Administration to mandate the deployment of this necessary equipment.

TRAVELER IDENTIFICATION AND AIRCRAFT SECURITY

To implement a broad system of biometric controls for air travelers, we propose a closer partnership between airlines, the FAA and Federal law enforcement authorities to implement programs for trusted travelers. The objective of this effort would be to streamline clearances for many U.S. citizens and others with proper documentation. The projects would have the effect of implementing the voluntary Travel ID Card proposal that was advocated by the Department of Transportation Rapid Response Team for Airports last month. Traveler participation would not be mandatory, and by law the program would not be tied to a specific card that could be demanded for purposes other than travel.

A first step would be to offer the new process to a traveler who possesses a government-issued identification document such as a U.S. passport, Permanent Resident Card, or other secure document defined by law. The applicant would enroll in the program through a participating airline. Biometric information would be captured from the applicant and securely stored for later use at locations such as check-in, security clearance, and boarding. The FAA or other appropriate Federal agency such as the proposed Transportation Security Administration would be charged with conducting checks against law enforcement systems, with costs for this activity to be paid by the traveler in the form of a user fee. Travelers who clear this vetting process would be given access to a streamlined security system with dedicated lanes and special handling procedures. To enable airline-related services to be offered using the same business processes, the participating airline would be responsible for issuing the card that would provide the link to the secure biometric information.

As noted by those who have supported the Travel ID Card concept, many details need to be worked out before all necessary elements of the system could be put in place. We recommend that this should be the responsibility of a Commission that would be appointed by Congress to promptly examine the issues and recommend specific legislation that would be required to implement the concept. Given the critical need for this coordinated effort, we recommend that the Commission, if authorized by Congress, should issue its report within 120 days of enactment.

This recommendation for a public-private partnership fits well with other cooperative efforts that are well underway. Notably, the multi-stakeholder Simplifying Passenger Travel (SPT) initiative sponsored by the International Air Transport Association also recommends the widespread use of biometrics for travelers. SPT programs should help the U.S. to identify a broader range of bona fide travelers who have been enrolled in biometric control systems that are implemented here and in other countries. Meanwhile, the International Civil Aviation Organization (ICAO) continues to make progress in standardizing the use and storage of biometrics on passports to make conterfeiting, identity theft, and imposter fraud more difficult for those will ill-intent.

Senator ROCKEFELLER. Dr. Yura, I hope that you will say some good things about West Virginia University here.

STATEMENT OF MICHAEL T. YURA, PH.D., DIRECTOR, WEST VIRGINIA UNIVERSITY FORENSIC IDENTIFICATION PROGRAM

Dr. YURA. Me too. Senator Rockefeller and Members of the Subcommittee, my fellow panelists, President Hardesty and guest colleagues and the significant technology expertise present here in this room, I really appreciate the opportunity to speak with you concerning biometrics and its role at West Virginia University. We greatly appreciate your interest in biometrics and the opportunity to share with you and the Aviation Subcommittee information about our efforts here in West Virginia.

I am currently director of the Forensic Identification Program for West Virginia University. The primary impetus for the development of this Forensic Identification Program that is here was that there were no programs like it, within the State of West Virginia, the United States, or throughout the world that specifically train individuals and grant degrees in the area of forensic identification. The Federal Bureau of Investigation——

Senator ROCKEFELLER. I'm sorry. Repeat what you said because you're speaking a little bit softly. I want to make sure you are clear. That the only undergraduate degree in——?

Dr. YURA. Forensic identification.

Senator ROCKEFELLER. Forensic identification offered in the country is offered here?

Dr. YURA. Yes, sir.

Senator ROCKEFELLER. And only here.

Dr. YURA. Yes, sir.

Senator ROCKEFELLER. That is pure propaganda.

[Laughter.]

Dr. YURA. The programs that we offer here are both in forensic and investigative science and biometrics. And the impetus for this program came from—at the request of the Federal Bureau of Investigation, seeing the void in terms of the training in technology and granting degrees in this area. Michael, Deputy Director of the division is here today, and we thank you for the insight that they had in recommending that these were technologies that need to be developed, and educational programs. We thank you very much for that.

Our biometric programs include areas of emphasis in sensors and circuits, signal processing, statistics, software systems, and DNA and molecular biology. These programs have begun to address the current and future needs of individuals with increased scientific expertise in forensic identification technologies and forensic sciences.

The use of advanced identification technologies for commercial, forensic, military, and security industries has created a significant need for scientifically trained persons with technical skills in computer science, engineering, biometrics, and the natural sciences.

The biometric program at West Virginia University is housed in the College of Engineering and Mineral Resources within the Lane Department of Computer Science and Electrical Engineering. This program within the forensic identification program is supported directly under the Provost and Vice President of Academic Affairs.

Just to step aside for a moment, the reason I am saying that is because President Hardesty and Dr. Lang took this program and said, this is a multidisciplinary program. It is going to be under the Provost's office so we can then stretch across the university and take the expertise from our medical center, from our arts and sciences, as well as engineering, and mold them together to fit the needs; which is I think a new concept and is working very well, and is a prototype for a new type of degree.

The biometric program efforts are supported by some significant honors and activities. WVU was recently listed as a Center of Excellence in Information Assurance Education by the National Security Agency. We were recently awarded money for student scholarships and the creation of a new laboratory in support of information assurance from the Department of Defense. We are also involved in the creation of a certificate program in Information Assurance and Biometrics for the Biometric Management Office of the U.S. Army as the lead agency in Biometrics for the Defense Department.

We have also developed a Memorandum of Understanding with the Biometric Foundation, a non-profit arm of the International Biometric Industry Association for the purpose of conducting cutting-edge research and development in biometrics for commercial and government applications.

Effectively addressing the breadth of biometric identification system research from the life sciences to the computing and statistical sciences represents a significant interdisciplinary challenge. The concept of our Center for Identification Technology Research, often referred to as CITeR, was developed by WVU with its academic partners to establish the first comprehensive academic center to serve the growing biometric identification technology research and education needs. While here at WVU, CITeR's organization is a virtual multiuniversity center, drawing upon interdisciplinary faculty expertise at WVU, Michigan State, Marshall, and San José State University in order to enable it to address every technical aspect of biometric systems, from sensor devices through software and systems. Dr. Larry Hornak, the director of that center is here with us today also.

CITeR was funded for planning, and its operational center proposal is pending with the National Science Foundation to become the first National Science Foundation/Industry/University Cooperative Research Center addressing the area of biometrics. The goal of CITeR and NSF is to serve the needs of its members by advancing the performance of biometric systems through cutting-edge research and enabling technology, interdisciplinary training of scientists and engineers, through its biometrics research, and the facilitation of the transfer of new biometric technology to the private as well as government sectors.

During the planning panel last April, there were programmatic areas where outlines—in the area of sensing and analysis, signal and image processing, pattern recognition, and statistical design. Out of that a list of studies currently on are listed. I will mention a few of them. A study on life detection in biometric devices; a study of multimodal biometric systems by Michigan State in cooperation with WVU; two collaborative projects between WVU and San José State seeking a mathematical framework for estimation of population sizes for biometric system testing; as well as a study of issues in large-scale biometric authentication infrastructure at WVU.

The Forensic Identification Program and its biometric information assurance program, as well as our broad activity in homeland security efforts in education, training, research, and development are at the disposal of any branch of the U.S. Government, as well as the critical industries such as the airline industry, in promoting passenger safety and preventing domestic terrorism. We greatly appreciate the opportunity to serve the people of the United States.

I would like to make one other additional comment. Your extensive involvement with the Veterans Administration, we feel in working with different groups to apply this same technology for the protection of medical records and we mentioned earlier, this is enabling technology. So not only are you talking about perimeter security and access, but also limiting the amount of people who have access to those records. We feel that it is really a critical piece of our broad mission here at WVU to support those efforts as well.

Senator ROCKEFELLER. And that is by knowing where anybody is at any given time.

Dr. YURA. Certainly, as well as identifying those persons who have the right to have access to that and limiting that information. Thank you, Senator.

[The prepared statement of Dr. Yura follows:]

PREPARED STATEMENT OF MICHAEL T. YURA, PH.D., DIRECTOR, WEST VIRGINIA UNIVERSITY FORENSIC IDENTIFICATION PROGRAM

Senator Rockefeller and Members of the subcommittee, I greatly appreciate the opportunity to speak with you concerning biometrics and its role at West Virginia. We greatly appreciate your interest in biometrics and the opportunity to share with you and the Aviation Subcommittee information about our efforts here in West Virginia.

I am currently the Director of the Forensic Identification Program at West Virginia University. The primary impetus for the development of the forensic identification program was that there is currently no program within the State of West Virginia, the United States, or throughout the world that specifically trains individuals and grants degrees in the area of forensic identification. The Federal Bureau of Investigation (FBI) in response to this major training and educational void requested that West Virginia University (WVU) develop degree programs in Forensic Identification with an academic major in Forensic and Investigative Science and Biometrics. The Biometric major includes areas of emphasis in Sensors and Circuits, Signal/Image Processing, Statistics, Software Systems, and DNA/Molecular Biology. These new programs will begin to address the current and future need for individuals with increased scientific expertise in identification technologies and forensic sciences.

The use of advanced identification technology for commercial, forensic, military, and the security industries has created a significant need for scientifically trained persons with technical skills in computer science, engineering, biometrics, and the natural sciences.

The Biometric Program at West Virginia University is housed in the College of Engineering and Mineral Resources within the Lane Department of Computer Science and Electrical Engineering. This program within the Forensic Identification Program is supported directly under the Provost and Vice President for Academic Affairs. The Biometric Program efforts are supported by some significant honors and activities. WVU was recently listed as a Center of Excellence in Information Assurance Education by the National Security Agency (NSA). We were recently awarded money for student scholarships and the creation of a new laboratory in support of Information Assurance from the Department of Defense. We are also involved in the creation of a certificate program in Information Assurance/Biometrics for the Biometric Management Office (BMO) of the U.S. Army as the lead agency in Biometrics for the Department of Defense. We have also developed a Memorandum of Understanding with the Biometric Foundation, a non-profit arm of the International Biometric Industry Association (IBIA) for the purpose of conducting cutting edge research and development in biometrics for commercial and government application.

Effectively addressing the breadth of biometric identification system research from the life sciences to the computing and statistical sciences represents a significant interdisciplinary challenge. The concept of the *Center for Identification Technology Research* or "CITeR" was developed by WVU with its academic partners to establish the first comprehensive academic center to serve growing biometric identification technology research and education needs. While based at WVU, CITeR's organization is that of a virtual multi-university center, drawing upon interdisciplinary faculty expertise at WVU, Michigan State University, Marshall University, and San Jose State University in order to enable it to address every technical aspect of biometric systems from sensor devices and biosignals through software and systems. CITeR was funded for planning, and it's operating center proposal is pending with the National Science Foundation to become the first NSF Industry-University Cooperative Research Center addressing the area of biometrics. The goal of CITeR as an NSF Industry/University Cooperative Research Center is to serve the needs of its members by advancing the performance of biometric systems through cross-cutting research of new enabling technologies, interdisciplinary training of scientists and engineers through its biometrics research, and the facilitation of the transfer of new biometrics technology to the private and government sectors through its membership.

During the Center's first Planning Conference held in April of this year at WVU and facilitated by the NSF, prospective center members working with faculty participants from the four universities defined CITeR's initial portfolio of research. CITeR's research activities and capabilities span four programmatic areas that cover the functionality of biometric systems. These four research areas are *Sensing and Analysis, Signal and Image Processing and Pattern Recognition, Statistical Design and Evaluation*, and *Biometrics in Information Assurance.* At the April planning meeting, nine projects were presented to prospective center members ranging from biosensors to automated dental record identification systems. From this set, five projects were selected to form CITeR's initial research portfolio. Briefly, these five are:

- *A Study of Liveness Detection in Biometric Devices* that will look at extending previous work at WVU in the area of spoof detection in fingerprint biometric systems,
- *A Study of Multimodal Biometric Systems* by Michigan State University looking at the optical design of systems using multiple biometrics,
- Two collaborative projects between WVU and San Jose State—one seeking to develop a mathematical framework for *Estimation* of population sizes for biometric system testing and the second developing the framework for a study of *Template Aging*, and
- A study of *Issues in Large-Scale Biometric Authentication Infrastructure* by WVU which explores the role of biometrics in the assurance of information in large-scale information systems.

The Forensic Identification Program and it's Biometric effort in education, training, research, and development are at the disposal of any branch of the U.S. Government as well as the critical industries such as the airline industry in promoting passenger safety and preventing domestic terrorism. We greatly appreciate the opportunity to serve the people of the United States.

Thank you.

Senator ROCKEFELLER. Thank you.

I want to go right back to something that was said here in West Virginia, and that is that small airports—and you mentioned international is the other. They are what we have. And we have more flights from some, very few flights from some. But they are us and they are many other States. So we treat them preciously. If you are given—and I do not know who I am asking this—if you were given a small airport, and let us say about 30- to 60,000 planes a year, and asked to deploy the best possible, cost-effective and available technology, what would you do and what would it be likely to cost to cover it?

Mr. PLANTON. I will start with that. We have employed EI situations in the Ben Gurion airport. We started with the prototype that took 90 days to implement and four kiosks. It is very scalable. And when you're talking about small airports and large airports, you are talking about scalability. A small airport might only take one kiosk, and we're talking in the 40,000 or more range. And then as we get to large airports, we scale the kiosks. That, coupled with the process at the airports, could secure that airport just as well as any larger airport.

Senator ROCKEFELLER. Then you better explain for all of us the full range of what a kiosk provides.

Mr. PLANTON. A kiosk is just what we build to put the biometric and smart card technology in. And it is demonstrated out in the hallway. What we do is, you put your smart card into the kiosk with your biometrics imprinted on the smart card. In Ben Gurion, there is hand geometry and facial recognition that will scan your face and your hand, match it with who you are on the smart card, and allow you to prove who you say you are.

That would be a known passenger who has already been through a background investigation so that we can move them through the airport expeditiously. What we want to do is take the known passengers everybody is talking about out of the mix.

If we have 100 percent passengers and we take 40 percent of the frequent flyers out of those lines and move them through and expedite them through the security process because we have already done the background investigation—we know through the smart card and biometrics on the smart card who they are—then we are going to benefit both the frequent flyers going through the airport, but we also reduce the line from 100 to 60 for the unknown passengers. Which are going to be let on the airplane if they pass the rigorous security checks, but they will take longer to do that.

In the airport in Israel, 15 percent of all passengers are now using the system to go through the airport. And instead of standing in an over-an-hour line, they can go through the security system in about 15 seconds.

Senator ROCKEFELLER. That's a big—it's a big deal, isn't it? In other words, for people to see it that way. On the one hand, it appears to be data going out of there; but on the other hand, instead of waiting for 2 hours, I can go through in 15 seconds.

Mr. PLANTON. We put the booths to enroll in sight with people standing in line, which promotes those people standing in line to go enroll. We also use the bank card technology now, so they will not have to carry multiple cards. Because if you see the credit cards coming out of our financial institutions are the smart cards, there is no reason for it not to be on the credit card also. And in carrying that, we allow them to go from their carrying one, to carrying the two cards, to putting it on their bank card.

Senator ROCKEFELLER. Yes, sir.

Mr. SIEDLARZ. Mr. Chairman, I think that was well presented here. I'd like to turn my focus to the last aspect of your question. You mentioned earlier today the situation involving coming through the Portland, Maine airport as opposed to JFK. And I think the thing that we to have to think about nationally is that anything you do with a small airport in West Virginia better be a small version of what you do in the big airports. Because to the fellows that we are really worried about, the ones who have found their way in through the system, they are traditionally going to use the weakest link.

To focus entirely on the convenience issue—which is not being suggested here, I understand. But If we focus entirely on this security issue and the ability to identify these people, we can focus on different solutions for the large environment, and certainly we have to address scale.

If we focus on different solutions for a variety of environments from big to small, then we are going have a system. There has got to be a compatibility in a comprehensive program and similarity in terms of what they encounter, what anyone encounters when they have to get through the air transportation system and how that system should be structured.

Senator ROCKEFELLER. And this is sort of an awkward question to ask, but I will ask it. If you were a terrorist, Mr. Siedlarz, would you not intuitively look for the weakest link?

Mr. SIEDLARZ. Absolutely. Absolutely.

Senator ROCKEFELLER. Why would you take on LaGuardia or JFK if you can take on a small airport?.

Mr. SIEDLARZ. That's precisely my point, Mr. Chairman. I mean, if you equip a tiny airport with a totally inadequate security system, they are going to find that airport. And they are not going to go through the big airport. Now, you might argue that well, for ports of entry or for crossing borders, you know, you can only go through a certain number of airports. But they are not all the same size either. And once again, you have to have some similarity in application and comprehensive approach or else you're going to have a flaw.

Senator ROCKEFELLER. And to follow on that, there was a point that I have made and others have made that one size doesn't fit all. That doesn't preclude the fact that inconsistencies of approach within airports dilute effectiveness.

Mr. SIEDLARZ. Absolutely.

Senator ROCKEFELLER. So in fact, I'm speaking against myself. In other words, not a one size, but a one approach or a one set of criteria eventually for all is, in fact, the only secure way to do it.

Mr. SIEDLARZ. Yes, sir. I think that you're talking about somewhat of a similarity integrated design. All details may not be the same because you have to deal with scale. And the cost won't be the same. But yes, there has to be a basic similarity in terms of the evenness, a level playing field with regard to security or else you are wasting your money.

Senator ROCKEFELLER. To any of you, I have this tremendous faith in biometrics, so I guess I am not a very objective or neutral person.

Mr. SIEDLARZ. You are perfectly objective.

[Laughter.]

Senator ROCKEFELLER. But explain to me, first of all the word iris, for example, has been used a lot here. And I'm trying to think of how long ago it was that I learned that the iris is the very darkest part of the eye, and the answer is not very long ago. And this is what I meant to be doing. So that this is new. Anything that is new scares people.

And particularly, there was one of the displays out there where you put your hand on something. I was very comfortable to do that, because what I found was, in fact, not just the nature—this was not just a fingerprint or a thumbprint, but it is my hand. And that is, if I had received, let us say, playing baseball or—that's not very good in my case—but something, a subskin wound 30 years ago, it would show up. It is there.

So it is another form of identification which nobody else can replicate except this particular hand. That gave me a feeling of security. Why is it, then, that biometrics, a new word—and it may not be—concerns people, if it does? As opposed to comforts people because it protects people.

Mr. SIEDLARZ. Well, as the industry guy, I will take a shot at that. And if I can, Mr. Chairman, let me correct a small inconsistency. People are confused between iris recognition and retinal scans. They are two very different things. The retina is the tissue in the back of your eye. You have to look through the pupil to read it. And the iris is not quite your definition. It is the colored portion that surrounds the pupil.

Senator ROCKEFELLER. Black.

Mr. SIEDLARZ. The black part is the pupil, and the colored portion that surrounds the pupil is the iris.

Senator ROCKEFELLER. OK.

Mr. SIEDLARZ. But more directly, I think it essentially comes from an unfamiliarity, with regards to the national view or people's view or the population view, unfamiliarity with biometrics. And it is remarkable in a way, because after all, one biometric, even though it has been done manually for a couple of hundred years, is the fingerprint, which almost everybody is associated with or is familiar with. What we have found in more recent years—and biometrics have been under development for some 25 to 30 years, as I mentioned earlier. But it did not reach great popularity until the last 10 years because of the cost and because of the reliability, both of which have been dramatically improved. And they are, in fact, proven systems today. This is not exploratory technology any longer. But not enough of the everyday public has seen the technologies in widespread deployment. When they have, I might add, in banking systems, in ATMs, things like that, they have accepted them. And in fact, the large majority have found them exciting and useful. And a means for avoiding carrying six or seven plastic cards and PINs and all these other things that you have to remember in today's complex society. So it is a selling campaign and an advocacy that is needed here to make sure they understand the true properties of the technology.

Senator ROCKEFELLER. We have, Mr. Planton and Mr. Selldorff, in West Virginia, both the research and undergraduate training which is being done here. And we have a testing facility run by the U.S. Army, a huge FBI center. It is not far away. We are a State which over the past 75 to 100 years has always been fighting uphill. Depending on natural resources and all kinds of things, our people have left. I remember 5 or 6 years ago was the first time in 40 years our population had not declined. It went up by a thousand. I rejoiced. That is what Las Vegas gets in an hour. It makes a difference to me. I was happy. And so if we have those types of capacities here, and in that two of the exhibitors outside, at least, are already doing business in West Virginia, should this not be an opportunity for West Virginia to tap, as they say—I hate the word, but, you know, leading-edge, cutting technology, which is of supreme importance to the security of the people of our country? Now, if that is not a loaded question, I have never heard one. But I am asking it nevertheless.

Mr. PLANTON. First of all, I married a girl from Parkersburg, West Virginia. Five girls and their mother were all graduates of West Virginia University. I spent a lot of time in section 227 at the stadium over there rooting for the West Virginia Mountaineers. So I'm very comfortable with this question.

You have started a program here with great insight into the future. Dr. Yura, you are citing the effect of technology, I think you were referring to, with the biometric security technology, with great insight also. And as a corporation, we are looking at that a lot. I believe that anytime you have a great research university like you have here, that is where technology starts. It is where it is tested. It is where it's fostered. It's where it's proven.

When we implement solutions, we are looking for proven technology, and it comes out of a university system. You have a great university here with great presentation. And yes, you should have high tech in this State in Morgantown, West Virginia. And, in fact, you do.

Mr. SIEDLARZ. I could only add to that, Mr. Chairman. I think the work that is being done by the university, by West Virginia University, is enormously important, not only for the industry. We should generally focus on the very small companies with very good technology, but who independently just do not have the resources and level of commitments in, other than spirit, to be able to achieve some of the end results that they would like to see with their technologies.

But working this in combination with a great institution like West Virginia, I think communicates a message to the people as well. It is not the message of just business trying to—or government for that matter—trying to translate to its constituency the value of the technology and getting over the technophobes and all the other things that they worry about. It shows that academics are appreciating and recognizing the important growth of an entirely new industry.

And at the same time, you know, creating the basis for the growth of that industry by providing the trained resources that we are going to need as it grows and as it goes forward.

Senator ROCKEFELLER. I do not even dare call on you, Dr. Yura.

Dr. YURA. I would like to make a comment if you do not mind. The biometrics as an enabling technology is exciting and the window of opportunity is tremendous. But whether in terms of airlines or other issues, the integration of these technologies is really critical. But my fear is that someone will just say I will just wrap this advice and we will take a piece of that, and it does not work because it is not integrated. And I hope in the future both airlines and others that—and of course, we at WVU would like to assist in that process, to make sure that these are integrated systems rather than just individual technologies. Because if they are not integrated, it gives biometrics a bad name that has nothing to do with biometrics. It is an enabling technology and in support, to make sure we really appreciate that.

Senator ROCKEFELLER. I understand that. But it also brings me back to an earlier point, and that is that when they talk about doing things on a voluntary basis, that is very comforting. It also means it is often very likely not to happen because of cost or inconvenience or somebody that was not aggressive enough. As opposed to causing them—and I never would use the word "mandatory" again since the Clinton health care bill.

[Laughter.]

Senator ROCKEFELLER. But I thought it was a good bill. And it brings the pressure—I mean, there has to at some point be a pressure, does there not, from the Federal Government as well as from others, from the industry in terms of, yes, making sure that we don't take a little piece here and a little piece there, but that we get after the business of doing it and deploying it all over the country, as they have in international airports. I mean, there is a kind of a fine mix here of making it voluntary so that we're not pushed too hard by it, or it costs too much for it, but also by saying this has got to happen. And we will not make the mistakes if we can possibly help it, but it has got to happen. So there is some balance there that we are in the process of still seeking.

Dr. YURA. One of the beautiful things, I think, about people in West Virginia, just as a group of individuals——

Senator ROCKEFELLER. I can't hear you very well.

Dr. YURA. One of the advantages, I think, of people of West Virginia in terms of doing things like this—if I pulled out my driver's license and I had my voluntary fingerprints in that driver's license. I think there is approximately 82 or 85 percent of all West Virginians volunteer to put their fingerprint on their driver's licenses.

Senator ROCKEFELLER. But at the same time, when you mention the concept of a smart card, there are a lot of people who say, now, wait a second. This automatically, then, becomes intrusive. And you are saying automatically it does not become intrusive. And so this dichotomy has to be dealt with, doesn't it?

Dr. YURA. Well, I think a lot of individuals who are concerned about safety and privacy issues and so on, that they recognize the need. I think there are a lot of people who would volunteer because of some of the surveys indicated by the earlier panel, and that's a start. And I think as we start, we'll have to move to a system people will comply with.

Senator ROCKEFELLER. And all of this within the context of the world did change on September 11, and will not be the same again for a long, long time.

Gentlemen, I want to thank you. I want to thank those of you who came here also with exhibits, which the public had a chance, and hopefully still has a chance, to look at outside. It is very, very appreciated. I think this is, in terms of aviation, a huge subject. And I think that generally in terms of technology and its role in how we conduct our lives in the future. And also information, availability of information versus the restrictions of privacy, and the tension between those two becomes very important. We do not want people coming from this country or into this country who should not be here and are here with—either here already or coming with malevolent intent.

And it is the government's first job and responsibility to protect the American people. That is absolutely—that is our basic responsibility. And on the other hand, we cannot—if somebody has, you know, diabetes and they are looking at trying to get a job, and all of a sudden that diabetes is revealed, and a potential employer sees that they have diabetes and says, well, you cannot have a job, we do not want that, either.

So we have a lot to figure out in a very short time in this country. You have helped us, and I thank you all very, very much. This hearing is adjourned.

[Whereupon, the hearing was adjourned.]

APPENDIX

PREPARED STATEMENT OF MARTIN HUDDART, GENERAL MANAGER, RECOGNITION SYSTEMS, INC.

Good morning. My name is Martin Huddart and I am General Manager of Recognition Systems, Inc. I am pleased to be here today to discuss technology innovations and solutions that can enhance security at America's airports.

Recognition Systems, Inc. (RSI) is based in Campbell, California, the heart of the Silicon Valley, and was founded in 1986. It is a pioneer in the application of biometric systems. Our primary technology is Hand Geometry. The company's HandReaders have been installed in high security environments around the United States and worldwide for more than a decade. Today, there are more than 60,000 RSI HandReaders around the world, reading millions of hands every day.

RSI is a subsidiary of the Ingersoll-Rand Company, a diversified industrial manufacturer and a world leader in security and safety. Together, IR and RSI provide integrated security solutions—including hardware, biometrics and electronic technologies, software applications, maintenance and consulting services—to commercial and industrial markets and customers in the United States and around the world. Our products, technologies and security solutions can be found in over 90 percent of the nation's nuclear power facilities, at major airports and other high-security environments, including prisons, military bases, sports arenas, hospitals, government buildings, border crossings and universities.

In the wake of the terrorist attacks on September 11, one task is certain: we must significantly increase and improve the security of our air transportation infrastructure, and we must do so quickly. President Bush and Congress have proposed a number of solutions, and much of the subsequent debate has focused on issues of how we can better professionalize and supervise security personnel at airports. These are important initiatives. But we should also recognize there is a critical role for technology to play in providing enhanced security at U.S. and international airports. This was endorsed by the Secretary of Transportation's Rapid Response Task Force on Airport Security, established in the wake of the September 11 attacks. The Task Force recommended in its report of October 1 that airports take immediate action to better incorporate technologies into security procedures used to identify passengers, airport workers and crews, and for improved detection of arms, explosives and baggage screening. The Task Force also recommended that the Federal Aviation Administration (FAA) establish a public-private sector consortium to identify, sponsor and test new security-related technologies for our nation's airports.

THE ROLE OF BIOMETRICS IN AIRPORT SECURITY

Biometric systems lie at the core of technologies that can provide improved security at U.S. airports. Biometrics is the science of using physical characteristics to identify an individual. Modern biometrics systems were developed in the mid-1970s. Early commercial products were expensive and therefore limited to very high security applications, such as nuclear facilities and laboratories. In recent years, inexpensive microprocessors and advanced imaging electronics have greatly reduced the cost of biometric devices, while increasing their accuracy. These changes have made biometrics increasingly common in commercial applications. Today, thousands of businesses from daycare centers to college dorms use biometrics for their access control needs, as well as for accurate personnel time and attendance monitoring.

Our hand geometry technology was specifically designed to be used in high-volume environments, where access must be tightly controlled and there is a need to provide forgery-proof identification procedures. Our technology has been engineered to work reliably in difficult security environments such as airports, which demand rock-solid performance even in outdoor applications. *The accuracy, reliability, durability and successful track record of biometric hand reading technology is unparalleled in the industry.*

Biometric hand readers simultaneously analyze over 31,000 points and instantaneously record over 90 separate measurements of an individual's hand—including length, width, thickness and surface area—to verify that the person using the device is really who he or she claims to be. The hand reader compares this information with a "template" of the individual's hand that has been previously stored in the reader, on a server or on a card. Once the person has been identified as a valid user, a door can be opened, or access can be provided to an air operations area or to boarding a plane. The reading and verification process takes less than a second.

PROVEN VS. EXPERIMENTAL TECHNOLOGIES

Members of Congress and Federal and local aviation authorities are presently being inundated with proposals for new technologies that can be incorporated into the nation's air transportation system. This includes many different biometric systems, including hand, iris, fingerprint, facial and voice recognition.

While there is no disagreement that technology can enhance security at our nation's airports, we must also understand this is not the time to experiment with new and unproven systems. *Only those technologies that have already been proven in the airport and travel environment, and which have an established reputation for reliability, should be in the forefront of our decision-making process as we consider how to proceed in the weeks and months ahead.*

Decision-makers must understand that the different biometric technologies being discussed in today's new airport security environment are in various stages of development and not all have the same record of reliability and performance. Hearings like this are important for policymakers in Washington and airport officials around the country to better understand the scope of existing and new technologies, and to see and compare first-hand the relative advantages and disadvantages of different technology solutions.

We also feel it important to point out that we should not be looking for the one biometric technology that solves all the identification needs of our transportation system. This does not exist; there is no silver bullet. What should be done is to take the best of breed and apply them appropriately.

RSI participated in a demonstration of biometric security technologies sponsored on October 27 by Rep. Jim Matheson (D-UT) at Salt Lake City International Airport, which will serve as the gateway to tens of thousands of U.S. and foreign visitors attending the Winter Olympic Games in February. RSI demonstrated how our biometric HandReaders, when used with smart card technology, can be an integral part of an airport's integrated security system.

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 airport environments for employee access and high volume passenger verification.*

It is important that the FAA, as the Federal agency with overall jurisdiction and responsibility for aviation security, take the lead in determining specific airport security technology standards to be adopted for individual airports. To facilitate this effort, Rep. Matheson and Rep. Mike Honda (D-CA) have introduced H.R. 3101, which would direct the National Institute of Standards and Technology (NIST) to develop standards and measures for aviation security technologies. The FAA would fund and carry out a pilot program in at least 20 U.S. airports to test and evaluate the effectiveness of various existing, new and emerging aviation security technologies, and then report on their findings and recommendations. These pilot projects will provide an opportunity to compare and evaluate different biometric systems.

We certainly support these pilot programs, but also know that they will take time. And time is our enemy. So we must have a short-term as well as a long-term strategy for the use of biometrics to enhance the security of America's transportation infrastructure.

THE SHORT-TERM GOAL: IMPROVED AIRPORT ACCESS CONTROL

The Federal Aviation Administration (FAA) already directs U.S. airports to insure that only authorized individuals are allowed access to flight operations areas. Most airports implement this directive by using card-based access systems to control access to high-security areas. However, card-based systems are an inadequate technology to control access. These systems can only positively or negatively identify the card, not verify that it belongs to the individual using it. By contrast, a biometric system can truly verify the person.

For 9 years, San Francisco International Airport (SFO) has been using RSI's HandReaders to meet the difficult challenge of securing access to sensitive areas of the facility. More than 30,000 airport employees are enrolled in the system which spans the entire airport and protects more than 180 doors. SFO has demonstrated the reliability of RSI's hand geometry technology in the airport environment over several years of use.

Using biometric hand readers to control airport-wide access not only enhances security, it provides confidence to airport employees by demonstrating that a major and obvious security need is being successfully addressed. It also increases confidence of the traveling public who can see this technology layer in place throughout the facility. This is not a pilot or demonstration project; it is a permanent, proven solution that lies at the core of SFO's security infrastructure. *Therefore, with confidence, we can deploy our technology at every U.S. airport now and the enhanced security we provide at SFO can blanket the rest of our nation's airports.*

To this end, current regulations governing access demand that only authorized people be allowed access. A clarification to this regulation (FAR 107.14a) is needed to ensure that it is being followed with the full and clear intent of the regulation, and calls for the use of biometrics to achieve this goal.

A LONGER-TERM GOAL: AUTOMATED AIRCRAFT BOARDING SYSTEMS

In the wake of September 11, Americans have experienced more complex and time-consuming security procedures at U.S. airports. Media reports have focused on passengers who have confronted long and slow-moving lines at airport security checkpoints. Most Americans recognize the need for new and improved security improvements and so far have been patient with the inconveniences they cause. But the reality is that the traveling public will soon demand ways to automate this new, higher level of security. This will be particularly the case with business travelers who need to fly frequently, and to whom long delays have an economic consequence.

One approach to this problem is for U.S. airports to segregate passengers into "high risk" and "low risk" categories. This allows airport security personnel to focus their time, attention and resources on a relatively small number of "high risk" passengers. By doing so, security processes can be eased for individuals who have been pre-determined to be at "low risk," and who make up the bulk of the traveling public.

This type of system has been in place for 7 years as part of a pilot program of the Immigration and Naturalization System (INS). It is called INSPASS. Frequent travelers have a background check performed and upon passage of this they are entered into the program. A kiosk at U.S. immigration control is used to allow the INSPASS user to insert their identification card and enter appropriate flight information. Their identity is then confirmed by using an RSI HandReader. The live template of the user's hand is instantly compared with the template that has been previously stored in a secured government database. If the templates match, the individual can proceed. Over 23,000 transactions take place each month at nine separate North American airports.

A similar program is in use at Tel Aviv's Ben Gurion International Airport, one of the world's busiest air terminals and a facility recognized and respected around the world for its high level of security. RSI HandReaders are used in a system designed by Electronic Data Systems Corporation (EDS) that allows Israeli citizens and frequent international travelers to use an automated inspection and identification kiosk. Travelers use a credit card for initial identification; then the system instantly verifies their identity with a HandReader. The system prints a receipt that allow travelers to proceed.

Ben Gurion's biometric identification system has reduced long waiting times at security checkpoints. The automated inspection and identification process takes about 20 seconds to complete. By contrast, passport control lines at Ben Gurion can take up to an hour. The project was initially offered only to frequent travelers, but has recently been made available to all Israeli citizens. Nearly 80,000 Israeli citizens have enrolled in the program, and the system is now processing about 50,000 participants each month. In 2002, a similar biometric border crossing system will be installed at the Israeli/Palestinian border to verify the identity of 50,000 people who cross the Gaza Strip every day.

Developing a similar system here in the United States was one of the core recommendations of the Secretary of Transportation's Rapid Response Team on Airport Security. The Rapid Response Team concluded "there is an urgent need to establish a nationwide program of voluntary, pre-screening of passengers, together with the issuance of 'smart' credentials, to facilitate expedited processing of the vast majority of air travelers and to enable security professionals to focus their resources more effectively." (Recommendation No. 16).

We are confident that a similar system could be developed for U.S. airports and the Federal Government and Congress should provide the leadership necessary to implement this concept. To this end, we recommend that the U.S. Department of

Transportation conduct a study of options for improving positive identification of passengers at check-in counters and border crossings through the use of "smart cards" and biometrics, in an effort to determine the feasibility and cost of such a program and a schedule for requiring air carriers to put it in place.

USING BIOMETRICS TO VERIFY IMMIGRATION AND VISA STATUS AT U.S. AIRPORTS

Biometrics can also play an important role in addressing shortcomings in the nation's immigration and visa systems. America's open borders have created ample opportunity for terrorists to enter the United States. Each year, more than 300 million individuals cross our borders. While for the most part these border crossings are legitimate citizens and visitors, the U.S. lacks the ability to track border crossings, or even to accurately confirm the identity of individuals entering or leaving the country.

Legislation introduced in the U.S. Senate on October 25 by Senator Diane Feinstein (D-CA) and Senator Jon Kyl (R-AR) seeks to improve the ability of immigration officials to identify foreign visitors at U.S. airports and other border crossings by using biometric technologies. The legislation would develop a new biometric "SmartVisa" card that foreign nationals would swipe upon their entry and exit to the United States. To ensure that these cards correctly identify the individual who is authorized to use them, the bill would authorize funding for INS to deploy biometric card readers and scanners at all U.S. airports, seaports and land border crossings.

Here again, a similar system is already in operation in Israel. The Israeli Government is using RSI HandReaders in its BASEL border-crossing project. Paired with Visionic's facial scanning technology, this dual biometric system is designed to verify the identity of more than 50,000 individuals who daily cross the Israeli-Palestinian border. In an area of the world where citizens live with the fear of terrorism every day, and where there exists a need to manage border crossings with extraordinary reliability and accuracy, the fact that the Israeli Government has chosen RSI HandReaders for this task should serve as a positive endorsement that this system represents the best available technology for use in U.S. airports.

CONCLUSION

As our Nation moves forward following the tragic events of September 11, the overriding security issue will be to better manage people and access within the complex environment of a commercial airport. Technology, even sophisticated biometrics, cannot replace improved training for security personnel and heightened human monitoring and vigilance. We know that even the most careful baggage screener can grow tired after hours on the job. And the most careful worker can mistakenly lose an ID card or a key. But a biometric hand readers will not fall asleep on the job; it will never take a day off; it won't allow airport employees to "piggyback" behind authorized workers; and it won't "loan" its ID card or access code to cousins, friends or co-workers.

For these reasons, biometric hand readers offer a valuable solution to enhancing security for Americans who depend on our air transportation system and who today, and tomorrow, need to be reassured that those charged with the responsibility of providing for the public's safety have evaluated and utilized every available technology to do so.

Thank you.