S. HRG. 107–1069

AVIATION SECURITY—NEXT STEPS

FIELD HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

DECEMBER 10, 2001

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

U.S. GOVERNMENT PRINTING OFFICE

89–684 PDF WASHINGTON : 2004

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii	JOHN MCCAIN, Arizona
JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska
JOHN F. KERRY, Massachusetts	CONRAD BURNS, Montana
JOHN B. BREAUX, Louisiana	TRENT LOTT, Mississippi
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
RON WYDEN, Oregon	OLYMPIA J. SNOWE, Maine
MAX CLELAND, Georgia	SAM BROWNBACK, Kansas
BARBARA BOXER, California	GORDON SMITH, Oregon
JOHN EDWARDS, North Carolina	PETER G. FITZGERALD, Illinois
JEAN CARNAHAN, Missouri	JOHN ENSIGN, Nevada
BILL NELSON, Florida	GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*
MARK BUSE, *Republican Staff Director*
JEANNE BUMPUS, *Republican General Counsel*

CONTENTS

AVIATION SECURITY—NEXT STEPS

MONDAY, DECEMBER 10, 2001

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Atlanta, GA.

The Committee met, pursuant to notice, at 10:16 a.m. in room 2306, Richard B. Russell Federal Building, Atlanta, Georgia, Hon. Max Cleland, presiding.

OPENING STATEMENT OF HON. MAX CLELAND, U.S. SENATOR FROM GEORGIA

Senator CLELAND. The Senate Commerce Committee will come to order.

We are delighted to have all of you present today. Let me just say that as a member of the Commerce Committee and the Subcommittee on Surface Transportation and the Subcommittee on Aviation, it has been quite a ride since September 11. Our transportation infrastructure has taken a hit, particularly our airlines. And this being the site of the busiest airport in the world, we wanted to come here and see how we were progressing and what we needed to do to stay on track with the new aviation security law.

One of the wonderful people we have with us today is Deputy Secretary of Transportation Michael Jackson. Michael, we are delighted that you came south and we thank you very much. Give Secretary of Transportation Norm Mineta our best regards. He has got a tough job and he is a distinguished American and a great friend. We would love for you to convey our thanks to him for letting you come.

I have a basic opening statement that I would like to share with you and then we will get into the testimony. We will try to conclude today by noon. We will ask all of our panelists to try to keep their remarks to about 5 to 8 minutes. We are not going to be too rigid in that regard because we want you to share with us how you are coming along. I would like to lead off by again giving thanks to everybody who came today.

We have on the books now a landmark aviation security bill that was passed originally by the Senate 100 to 0, which is a historic moment in and of itself, and a bill was later passed by the House. The conferees basically adopted about 98 percent of the Senate bill and it was signed into law by the President. This historic piece of legislation was enacted in response to the events of September 11 when, as you know, terrorists commandeered U.S. commercial jets filled with passengers and used them as weapons of mass destruction.

It was an act of war on America's citizens. On that day of infamy, there were more casualties at the World Trade Center, the Pentagon and on the four hijacked jets than there were at Pearl Harbor.

The terrorist attacks of September 11 have precipitated a sea change in attitude on how we view our homeland security. Homeland security, aviation security are now part of our national security. There is no such thing as business as usual any more.

Immediately after the events of 9/11, the Federal Aviation Administration and the U.S. Department of Transportation took steps to tighten aviation security around the country. U.S. airlines and airports put in place security safeguards and Congress passed the most sweeping aviation security bill in history.

Every commercial airport will now have a Federal security manager and the manager will conduct an immediate assessment of safety procedures at the busiest airports in the country. We will have strict uniform national standards for the hiring and training and job performance of the men and women who are on the front lines of ensuring that our airports and airplanes are not only the safest in the world, but also the most secure. Because of this legislation, every airport screener must now be a U.S. citizen. He or she must pass a criminal background check and he or she must perform well in their job. If they do not, they can be fired immediately.

Cockpit doors are already being fortified. The number of air marshals on airplanes are already being increased and international flights are now providing the U.S. Customs Service with passenger lists before they can land in this country.

Testifying today will be Deputy Secretary of Transportation Michael Jackson, the No. 2 official at the Department of Transportation. Until the new Under Secretary for Security is sworn in, Mr. Jackson has oversight over the security of our aviation system. I might add that Mr. Jackson once taught political science at the University of Georgia. Go Dogs!

[Laughter.]

Senator CLELAND. Therefore, he will have a bulldog approach to security.

[Laughter.]

Senator CLELAND. Today, the Committee will hear from the Deputy Secretary on the national status of our aviation security in light of the September 11 events, how the new aviation security law is being implemented, and the transition challenges we face.

We are also fortunate to have panelists from Georgia Tech and EDS, who will discuss the latest technologies to shore up security throughout the entire U.S. aviation system, from cockpits to off-limits airport areas.

Hartsfield, the world's busiest airport, Delta with its world headquarters in Atlanta and AirTran are key not just to Georgia's economy, but to our national aviation system as well. We will hear from panelists from each of these Georgia giants, who will tell us what security measures they have put in place since 9/11.

I will caution that our panelists cannot divulge certain information about measures they have already undertaken and will undertake which could compromise national security by benefiting those who wish America harm.

Representing Hartsfield will be its General Manager Mr. Ben DeCosta, who will address the incident of November 16 when an individual breached security at the Atlanta Airport. The security breach triggered the total evacuation of Hartsfield and a temporary halt of incoming and outgoing air traffic. That action caused a ripple effect of delays and flight cancellations. I might add that I have first-hand knowledge of those delays since I spent some quality time on the tarmac of about three and a half hours marooned along with 60 other aircraft due to this incident. It was a scary time; the initial reports were that the individual had a gun. We were all on the tarmac there, no aircraft was allowed to leave Hartsfield or to be boarded at Hartsfield. The only aircraft allowed to land at Hartsfield were those running out of gas. It was a very tense time. We forget that, but I can remember being in that aircraft and we all did not know exactly what was happening until hours later.

I would like to stress that despite those delays, the system here at Hartsfield worked. Hartsfield correctly followed the FAA directive put in place after September 11 that required airport lockdown until airport security could be assured. The November 16 incident revealed a glaring loophole in the system: an intentional security violation aboard an aircraft actually is a Federal crime. But a willful breach of an airport security checkpoint is punishable only by local criminal penalties and Federal civil penalties.

Just as we have at last stepped up to the plate to assure greater uniformity and greater accountability through Federalizing the airport security workforce, I believe it is the responsibility of Congress to address this shortcoming in our Federal laws. Accordingly, later today, I will introduce legislation to make willful violations of airport security checkpoints a Federal crime. We should send the message loud and clear that airport business is serious business, that if you come to a U.S. airport for mischief or for folly, you will pay the consequences. During this hearing, I hope to get input on my bill from our panelists and suggestions on how we can best deter such action in the future.

We have an outstanding line up of panelists today who are here to address the all-important issue of aviation security which, as we have recently learned in the most painful way, is a matter, as I said earlier, of national security.

I look forward to the testimony of our distinguished panelists and I would like to now recognize the Honorable Michael Jackson, Deputy Secretary of the U.S. Department of Transportation.

Mr. Jackson, welcome.

STATEMENT OF MICHAEL P. JACKSON, DEPUTY SECRETARY OF TRANSPORTATION, DEPARTMENT OF TRANSPORTATION

Mr. JACKSON. Senator Cleland, thank you for making me welcome. It is great to be back in Georgia and I will try to combine the bulldog determination with a little bit of that technical ingenuity that Georgia Tech is famous for and get a well-rounded approach to these aviation security issues.

Senator CLELAND. That is a good political answer.

[Laughter.]

Mr. JACKSON. I learned quickly from you, sir.

Senator CLELAND. That is right.

Mr. JACKSON. Senator, what I would like to try to do today is just do a quick overview and with your permission, I would like to submit my prepared remarks for the record.

Senator CLELAND. No objection, so ordered.

Mr. JACKSON. Then I will talk about two things—just a summary of the points that you made and one layer of more detail about the measures that we have taken since September 11 to improve aviation security, and then talk a little bit about how we are going to implement this new landmark legislation on aviation and transportation security, and be happy then to answer any questions that you might have about the particulars.

Last week, President Bush visited the aircraft carrier Enterprise to thank some of our men and women in uniform for the job that they were doing on the anniversary of Pearl Harbor, when he remembered service to our country of the World War II generation, and he said, "We are commissioned by history to face freedom's enemies." And Senator, I think you are absolutely right to say that the war against terrorism is ongoing and will be fought across transportation network of aviation and other transportation modes to make sure that we protect the country against the type of incursions that we witnessed on September 11.

I would like to tell you just briefly, to reinforce what you were saying, that we have put in place since September 11 very dramatic efforts to improve aviation security. This new landmark legislation, which the Commerce Committee pushed forward and advocated, is a substantial set of tools which will increase our capacity to improve transportation security. We must do two things. We must have world class security and world class customer service. We have to be able to make the airline system work well for the passengers. Our customers, as we launch this new system of aviation security under Federal management and with Federal employees, must understand that the taxpayers who are using the airline system are our customers and we are committed to providing world class security without compromise, while trying to make certain that we move the system in an effective and safe, efficient fashion.

Right after the events of the 11th, we did a series of things, really putting into place over 50 specific actions over the course of several weeks. On the first afternoon when the Secretary of Transportation ordered all of the aviation system down to the ground and stopped, to protect and assess what we were facing, we faced a series of incremental steps to put our system back together and put it up in increased security. And over the last 3 months, we have repeatedly added measures and assessed the ones that we initially deployed.

I believe that the airline industry did a magnificent job that day and I would be remiss not to say today that the industry, the men and women who worked on the airplanes, who worked on the ground to make that work efficiently, were real heroes that day also and I certainly believe that the air traffic control staff at FAA worked in great harmony with them to do the same.

So after we got them down, to get them back up and do it with enhanced security. We fundamentally put in place measures that worked with airports and with airlines.

Let me say just a little bit of an overview about some of the highlights of both and then we will—I would be happy to answer any questions about specific measures as I go through it.

On the airport side, we basically took the passenger—a process map of the passenger experience at the airport and looked at each point of entry and along the way introduced measures that would tighten up and strengthen security. We put manpower, technology and processes in place to increase security at airports. We worked with our airport partners who helped us figure out how to do some of these things in a more effective fashion and we have refined the tools that we initially put in place over the last several months.

At the checkpoints where you come in, there are new measures. On the ground, to provide a barrier against possible bomb, we created a zone. We limited and then refined the process of using curb side check-in. We have placed limits on checked bags and the processes that we are using to move them through the system. We have put a significant number of process changes in at airport checkpoints, at checkpoints where we move passengers through the screening process, new staff from the airlines, National Guard deployments, new procedures to be used and new tools to be deployed at those checkpoints.

In the restricted areas of the airport and the secure zones, we have put a whole series of processes in place to manage the security operation more effectively, including screening at the baggage points and screening at the gates of departure. So we have gone back behind the scenes of airport operation and done a variety of other things as well. We have put restrictions on the people who work at airports, they must go through the same check-in process and screening process. We put in place new rules substantially to enhance the background checking that is conducted and required for working at airports. We have looked at vendors who service airplanes in catering and other services and provided stricter controls over access.

We have looked at a variety of things on the aircraft themselves and the airlines have really done terrifically well at the door hardening exercise of putting bars and locks on doors to provide that strong barrier against incursions through the cockpit.

So with a variety of these tools, we have tried to reinforce, enhance, improve aviation security. There is much work to be done still. We have this new tool of the Aviation and Transportation Security Act to help us. So maybe I could take just a few moments to explain what this Act does and how we awre proceeding to implement it.

Essentially, the Act provides a new Under Secretary of Transportation reporting directly to Secretary Mineta the tools and the resources to Federalize the screening process for passengers and bags at 429 airports nationwide. We are going to put into place a substantially enhanced team of people and a substantially enhanced technology deployment to look for explosives and to test access to the secure zone and to the aircraft. We are going to continue to put money into technology innovation that will strengthen the cockpit security on board and we will have broad authorities granted to us by Congress to regulate the safety and security of the aircraft and the airports.

So this is a very large undertaking. As you know, Senator by the end of next year, we will have deployed at airports nationwide this new Federal force and we will have put a considerable amount of new technology into improving airport security.

Let me talk just a moment about how we are going to try to do that. First, there is an important point about how we are going to take this in a deliberate fashion, but a fashion that understands the urgency of what we have to do. We are going to pull together from the private sector, from across the Federal Government and from within the Department of Transportation the best minds tehat we can find. We have been planning and putting in place a transition team since before passage of the legislation so that upon its passage, we would have the tools and the process to handle this.

We have organized and put in place some process management techniques that have been used in the private sector continuously with large corporations and in some of the large deployments of forces in war time and peace time in the Federal Government. As you know, this is an unprecedented deployment of many, many thousands of individuals to airports around the country, but we have put in place a very firm process of how to do it.

I would like to describe just a few components of that process, if I could. First of all, the leader of this team on a day-to-day basis will be the new Under Secretary for Transportation Security and the Secretary and the President are working closely and with great focus on getting us a fine individual to run this new operation.

In the meantime, we have established a war room with a process executive that we have appointed to manage the overall processes that we have put in place. We have a series of about a dozen go-teams that are looking at specific problems. For example, how do we get explisive detection machines into airports in the 1-year time period provided for by the law. There is not enough of them if we just manufacture them in the current process, and putting them in is a complex process as well. So we have borrowed some folks from some of the Defense Department agencies who have done this type of work, we have borrowed folks from the private sector, we have taken a team of people internally and we are mapping out that process right now.

Similarly, there are about another eight to nine to ten of these go-teams working on various aspects of significant problems or issues that must be captured and dealt with quickly.

On top of that, we are using classical process mapping techniques to look at four categories of vulnerability—the passengers, air cargo, facilities and people who work in the facilities. So what we will do is we will map out from the time someone makes a reservation on the process side of passengers, for example, to the time that they finish their trip and we look at each point along the way from the reservation system to the arrival at the airport, check-in, screening, departure at the gate, experience on the airline. And we are putting in place tools and staff to address the vulnerabilities at each point along that process map. Then we will go to airports around the country with that basic process map and look through the specifics of that airport and make certain that we have refined it, adjusted it and worked it.

I had the pleasure of spending several hours last night at Hartsfield, it is my second trip to Hartsfield within the last 4 or 5 months and we had a terrific walk-through of security challenges and processes and issues there. We are going to be mapping that type of process all around the country.

I think one of the cornerstones as we take on passengers, cargo, people who work at airports and the infrastructure is going to be something that you mentioned, Senator, the Federal security managers. Federal security managers are the person representing the Federal Government at each of these airports that owns in their guts, in their hearts, in their minds, the security requirements that the Federal Government must address. We have some terrific people working for us in the FAA who are doing these jobs today, but we will be competing as we move into this new environment with Federal management for the best people possible to put in each of these airports and we will be training them carefully and supporting them with tools to make this work.

I would just say one last thing, try to talk about at the highest level how we manage this transition. We are looking at it really in three phases. In the first phase, we have, through the early part of next year, essentially the ongoing operation managed by airlines who contract out to third parties for security at airports and this process worked on conjunction with the ongoing responsibility for airport authorities.

In a second phase, beginning late January and proceeding for several months, the Federal Government will literally contract with those same third parties. No one is guaranteed to have the same job, you have to prove that you can meet the Federal standards. But we will have Federal officials overseeing these third party contracts. We will put in place new training requirements, we will put in place new eligibility requirements for people who are going to be hired after that transition period. And we will work through, during those several months, a transition to the third phase in which we deploy Federal workers to manage these jobs.

And so with this broad overview we will be managing the transition from what we have today to the new and substantial responsibilities we have ahead of us.

Senator, I look forward to working very closely with the Committee and with you personally as we manage this transition. We are committed to these two twin goals—world class security, world class customer service. We can do this, it is not easy, but we are going to do it and we are going to nail it just right.

[The prepared statement of Mr. Jackson follows:]

PREPARED STATEMENT OF MICHAEL P. JACKSON, DEPUTY SECRETARY OF TRANSPORTATION, DEPARTMENT OF TRANSPORTATION

Senator Cleland and Members of the Committee: It is a pleasure for me to be here in Atlanta today; I was given a very special tour of Atlanta's Hartsfield International Airport after I landed there last night, and was particularly impressed with the baggage operations at the world's busiest airport. These are quite impressive, and will serve as a model for us.

My statement today is devoted to the most pressing issue facing the Department of Transportation today: security, particularly for our aviation system. To describe our ongoing and planned efforts in this area, I have organized my statement as follows:

• A description of the actions we have taken in the wake of the tragic events of September 11 to immediately improve safety throughout the Nation;
• A description of how we are responding to the Congress' leadership in passing landmark aviation and transportation security legislation, and are already implementing key provisions of that Act; and
• An overview of our approach to standing up the new Transportation Security Administration (TSA), a massive undertaking that will require a sustained effort for at least the next year.

ACTIONS TAKEN IN THE WAKE OF SEPTEMBER 11

The tragic events of September 11, in addition to being an attack on our very way of life, were a multi-pronged assault on a critical component of our economy: the Nation's air transportation system. To restore confidence in the system and provide a safe environment for the traveling public, the Department, under the leadership of Secretary Mineta, took the following actions immediately to improve security at our Nation's airports and airlines:
• Increased patrols on and around airports;
• Increased terminal inspections, typically using highly trained canine teams;
• Instituted more intensive random ID checks throughout the airport: at the ticket counter, the screening checkpoint, and the departure gate;
• Increased monitoring of vehicular traffic and removal of unauthorized vehicles;
• Allowed only ticketed passengers and authorized individuals beyond screening checkpoints; and
• Instituted a zero tolerance policy at all security checkpoints, a policy that resulted in the intensive precautions taken here at Hartsfield a few weeks ago.

In addition, we have tightened our security procedures with respect to the Nation's air carriers in the following ways:
• Steadily increased the number of Federal air marshals on domestic flights;
• Adjusted CAPPS criteria for more intensive screening of all passengers to identify potential threats;
• Discontinued off-airport check-in;
• Required thorough inspection of all employee IDs;
• Required thorough inspection of all aircraft, including the interior and the galley, each day before passenger boarding begins; and
• Imposed new restrictions on jumpseat flights.

In the wake of Sept. 11, we also sought and received advice from experts in the fields of airport and aircraft security, law enforcement, and airline and airport operations—the Secretary's Rapid Response Teams. These efforts resulted in two reports—reports that identified critical areas where DOT should focus its attention and which provided specific recommendations as to how aviation security could be improved.

DOT ACTION ON KEY PROVISIONS OF TRANSPORTATION SECURITY LEGISLATION

As you know, the recently enacted Aviation and Transportation Security Act requires the Department to not only stand up a new agency, but also to make significant changes in our method of securing the Nation's transportation system. The Act provides great new tools to accomplish this, and to that end we have taken the following steps in the 3 weeks since President Bush signed the bill:
• Reduced operational access points at airports;
• Added Federal law enforcement officers at airports;
• Overseen a large deployment of National Guard troops at more than 400 airports;
• Increased distribution of name alerts;
• Required continuous use of all hand-wand metal detectors, explosive detection systems, and hand-checking of baggage, which means that even passengers not selected by CAPPS are subject to random search;
• Strengthened cockpit doors on nearly the entire US fleet, and put in place additional procedures to guard the flight deck; and
• Issued a final rule requiring all individuals with access to secure areas of airports, all screeners and all screener supervisors to be fingerprinted and undergo a criminal history record check if it has not been done in the past; and
• Established a link to the Office of Homeland Security and other Federal agencies to assist us in protecting the aviation system.

In addition, (1) we are close to completing the development of improved qualifications and training for screeners that will immediately improve security and form the basis for hiring high-quality TSA screeners next year; (2) we are working closely with the Nation's airlines to put a system in place for screening all checked baggage

by mid-January, as the Act requires; and (3) we are assessing the airlines' current contractual arrangements with screening companies so that we may assume this responsibility on time next February.

STANDING UP THE TSA

The job of standing up the TSA, a new Federal agency that will have sweeping powers, more than 30,000 employees, and the mission of protecting the Nation's entire transportation system, represents an almost unprecedented undertaking. As you would expect, President Bush, Governor Ridge, and Secretary Mineta have taken intense interest in the work we are doing. I would like to take this opportunity to briefly describe that work.

Secretary Mineta has appointed me to head up a special task force charged with standing up the new agency, identifying all of our statutory requirements, and developing a modern approach to securing the transportation system. To complete the thousands of tasks that must be undertaken to open the doors of the TSA next year, we are following a time-tested process management approach that successful private sector companies around the world use every day to execute large-scale transactions, mergers, or critical activities. This approach has the following important attributes:

- It enables us to prioritize our work according to the real-time needs of the system and the mandates of the statute: we have formed teams consisting of the leading experts from inside and outside the government to address issues on a very short timeframe, such as the 60-day checked baggage requirement;
- It allows us to develop a structure for the new agency that meets the needs of all the actors in transportation, at every level of every organization, and at every site in every mode: we have started now to develop plans for recruiting, hiring, training, and deploying thousands of screeners, Federal agents, air marshals, and other critical players;
- It keeps our focus on the most important aspects of transportation security and the agency itself—processes and functions: techniques are in place to develop processes targeted to optimum protection of the transportation system, while ensuring that every function required of us, and even some that aren't, are included in the TSA.

I would like to take this opportunity to say that restoring the public's confidence in the safety of our transportation system, and taking the necessary steps to promote and sustain safety over the long term is an open, inclusive effort that will consider, first and foremost, the requirements of passengers and industry, and will solicit the input of all who wish to contribute. In fact, a key aspect of our day-to-day operations is our cooperation with industry and communication with the Congress.

It is important to reiterate as well that the Government's efforts are not just the work of one agency—far from it. For example, in just the few weeks since the bill was enacted, we have already solicited the assistance of the Departments of Defense, Justice, Treasury, the Office of Personnel Management and, of course, all parts of the Department of Transportation.

In closing, let me say that although we have all been deeply impacted by the events of September 11—a direct hit on the transportation system we work every day to improve—the Federal Government, led by the Congress, President Bush, and Secretary Mineta, has risen to the occasion. I have tried to capture this response in my testimony here today, and look forward to discussing it further should you or other Members of the Committee have any questions. Thank you for your time and for hosting me in this great city.

Senator CLELAND. Well, thank you very much, Mr. Jackson, I appreciate that. I think that is a very positive and healthy attitude—world class security and world class customer service. You know, the airlines are in the customer service business. They are in the security business but they are also in the customer service business. One of the reasons I supported the federalization of the checkpoints, the 700 checkpoints at those more than 429 airports, was the professional level that we could get nationwide, a uniform professional standard.

I have also recommended to Secretary Mineta and to the President in several letters—and I will mention to you today—to consider a very great asset to the Federal Government, here in Georgia, in terms of training Federal law enforcement officials. The

Federal Law Enforcement Training Center, better known as FLETC, is down at Glynco, down in Brunswick, Georgia. They train Secret Service people, they train Customs people, they train Border Patrol. They are the world class facility for training Federal law enforcement personnel. And I've suggested in my correspondence to the President and to Secretary Mineta that they either have those airport screeners trained there or train the trainers there, so then you could send those out around America to train the workforce. The point is, I think you have a built in asset here that I just recommend that you seriously consider it, because those people every day focus on training Federal law enforcement personnel and they have for years.

Also, that center is familiar with the intricacies of all the other Federal law enforcement personnel that are out there, which is the point of one of my questions here.

In the scenario of attacks, a terrorist attack, biological attack, one of the things I am picking up on the Armed Services Committee and on the Governmental Affairs Committee and in testimony by Senator Nunn when he talked about his participation in an exercise called Dark Winter which was run by Johns Hopkins in June about a smallpox attack on America, that in the early phases of an attack, it is somewhat, shall we say, bureaucratic chaos. That the challenges are coordination, cooperation and communication.

I hope that in this legislation, we have outlined layers of authority and established in effect a protocol so that the system can deal with an attack or a breach of security and so forth. In other words, when something happens, everybody knows what their role is. The problem with say a terrorist attack or a biological attack or chemical attack is there is certain chaos if you do not have an established protocol. Now there are 60 different agencies as a minimum in the Federal Government that are in charge of, in effect, a piece of homeland security. We are just zeroing in on one of them here—aviation security.

But in that Federal security manager at the airport, I am kind of curious—and you may not be there yet in your mindset—but it does help, and one of the principles of war I have learned through the years is unity of command, that when something bad happens, people know what the chain of command is, they know who to go to, they know who to report to, they know who to communicate with, coordinate with and so forth.

In your mind, do you see that Federal security manager at airports in America in charge of other Federal entities? Here at Hartsfield, we have got INS, we have got the Customs Service, we have got the FBI, you know, we have a lot of folks in addition to the APD, the Atlanta Police Department. So at least there is a large Federal presence here. Do you see that Federal security manager, if maybe not in charge, then at least the lead dog, the team leader that when something happens, the protocol is established that that person is immediately notified and everybody knows that that is the person to go to and then there is a protocol established as to who does what to whom.

But I suggest that to you because in this whole world of response, one of the things I have learned is if there is unity of com-

mand and coordination already established in a protocol, that people know what to do. How does that match with some of your thinking about the role of the Federal security manager, who is a DOT employee answerable up the chain to the Deputy Secretary for Transportation Security?

Mr. JACKSON. I think you have got the same vision that the Secretary and I have as well, that this job is unique in that it must not only coordinate the security operation of the airport, but it must help us draw together all the Federal agencies who are working with the airport and to have this unity of command. It does not mean this person is going to be in the chain of command of the Customs Service, but it means that at the airport, this individual has to make certain that the Customs Service is able to have the type of access and have the type of plan necessary to react and that it is coordinated well with all the rest of the components of the Federal Government working at airports and with our local colleagues who are managing the airports and the airlines who are operating their networks out of these airports. So it is someone who must be—I am afraid I have to confess this one—this one has to be a bulldog in this process. They have to say I have it on my plate to understand the full spectrum of things.

I will tell you that since the events of the 11th and the creation of the Homeland Security Office at the White House, I have seen a tremendous amount of coordination. I have worked for three Presidents now and four Cabinet Secretaries and had a stint in the White House, and the cooperation among agenciees that I am seeing in these last few months is very intense and just unparalleled in the experience that I have seen in the executive branch. People are really working together. I will tell you just one short example of this. After the events of the 11th, we needed to expand dramatically our Federal air marshal program to put armed, undercover, trained agents in the air. And we borrowed professional law enforcement officers from all around the Federal Government—from Treasury, Customs, Secret Service, from the FBI, from Inspector Generals, from Fish & Wildlife, people who were trained and qualified to use firearms. So we are seeing tremendous cooperation. We have work to do to make sure that the chain of command scenarios are in place so that everybody knows how to pass information in the event of an incident.

I will just say to you that FLETC is a part of our plan to be able to train and deploy the large number of Federal law enforcement officers who will be working at airports and the Federal air marhals that will be flying in aircraft. They have tremendous experience and talent and I met last week with the senior Treasury Department officials who oversee that program operation. We have had numerous meetings with FLETC, they are part of the team.

Senator CLELAND. That certainly is good to hear. I have been down there and they are just a great national asset.

Mr. JACKSON. That is a fact.

Senator CLELAND. And one that I think an agency like yours in a situation like this where you have to ramp up so fast, that you need the best and the brightest that have been doing it a long time, then I commend them to your attention. I appreciate your meeting with them.

One of the things I would like to commend you on is your concept of multiple points of security, we will call it. I have had briefings—we have had briefings on the Commerce Committee from El Al and their whole concept of security—airport security, aviation security—has to do with layers of security, like peeling an onion.

Mr. JACKSON. Yes, sir.

Senator CLELAND. Starting, shall we say, at an outer perimeter and working more and more inward to, in effect, that moment when that individual boards the aircraft. And in your description of some of your own analysis of the pressure points, the checkpoints, where are we the most vulnerable, where do we need to strengthen.

And I think that layer of security concept will really give us the redundancy that we need. As a young Signal Corps lieutenant going on active duty in the Army in the mid-1960's, I had a Colonel tell me something very wise. He said, "Cleland, the secret is the reliability of redundancy". So in many ways, layering security, not just duplicative security, but layering various checkpoints, seems to be a concept that appears to work. El Al is a small airline. Our challenge here is a huge country, a huge aviation community and as of September 10, 650 million passengers a year and growing.

Mr. JACKSON. Yes.

Senator CLELAND. We had testimony earlier this year that we were going to have a billion people—a billion passengers flying in the next 4 or 5 years. Up until September 11, the challenge was where to put them all, enough air space, enough air traffic controllers, enough aviation traffic systems, enough capacity on the ground to handle it.

But I will say that I think the key to confidence in flying again is the extent to which we are able to be successful in our security. I say we, now that aviation security is equivalent to national security, and now that in effect we, the Federal Government, are in charge, I feel like I am part of your team as well.

Mr. JACKSON. I feel that way too.

Senator CLELAND. And I hope so. We on the Commerce Committee take our oversight role very seriously, which is one of the reasons why we are having this initial aviation security hearing.

Let me just ask you, talk to me a little bit about your understanding of how technology can help facilitate security. Obviously we have a greater role in terms of security, various checkpoints, layers and so forth; yet, there is technology out there that can expedite, speed up lines, waiting, whatever, pre-existing IDs, counterfeit-proof IDs, various things. Just tell me a little bit about some of the things that you are initially exploring in terms of technology. We have some examples of technology facilitation out in the lobby, but tell us a little bit about what you are looking at.

Mr. JACKSON. Well, I visited with interest the display of technology that we had out here with us today and the range of things that we are looking at is extraordinarily broad. We have put out a special request from the Department asking for technical ideas that can address various component parts of this problem and we had over 500 really top-notch ideas from major corporations, from individuals who had a great idea, and everything in between. They were for security screening devices, they were for biometric device

deployment, they were for tools that we can use on board airplanes to increase the security of cockpits and the security of the flight crews that work aboard our aircraft.

So we are really not stopping anywhere, but assessing around the globe and across the country what the best minds can bring to the table. We have a short-term job to do, but we are not looking at this as just deploy forces and get it over with and sigh and say, "Oh, I did my job, I checked my box". That is not our attitude at all. We are in this for the long haul. The threat is here for the long haul. We want to innovate aggressively but intelligently, we want to spend the taxpayers' money wisely, we are going to be spending an awful lot of it.

So the technology component is just an indispensible portion of what we have to do to provide this what we are calling systems of systems, the integration of multiple redundant and useful systems along the way that will increase the probability that the bad guys are not going to be able to do their work.

Senator CLELAND. Let us talk about identification of the bad guys. One of the reasons that I supported a national professional, in this case Federal, system was because it was obvious that aviation security and national security were inextricably linked and that in effect our Federal management of aviation security had to be linked into an intelligence data base that in effect was an early warning system. If Interpol picked up something in Stockholm, then we in Atlanta were ready for them when they landed here, or at least on the alert and that when they started coming through the system, then the professional system began examining and tracking this person.

My understanding is that under the new law, we run a background check on international passengers through the Customs Service.

Mr. JACKSON. Right now, we have already implemented early the provision that you are speaking of, which requires passenger manifests to be provided to the Customs Service in advance of passengers arriving for a flight into the United States. And the Customs Service is then able to take an integrated watch list and compare the passenger manifest against those watch lists. So that has already been implemented by the Customs Service in conjunction with this series of measures that the Congress has authorized.

We had earlier at the Transportation Department, early afterwards, looked, for example, at the flight deck crews of foreign registered aircraft coming into the United States and have put in place some additional measures to be able to make sure that we know who are flying the aircraft into the United States, what their background is, establish their credentials and to work through that. Some of the work in this area is something that I could not talk about in an open forum, but it is to say that we are looking at the full spectrum of passengers and crews as we bring this new security system on line.

We are also, I think, working much more focused with lessons learned from the 11th, to integrate various different watch lists and data base of information, data bases of information, from agencies, both domestic and from our allies abroad.

Senator CLELAND. Thank you. I understand that the new law directs the head of the FAA to establish pilot programs in at least 20 airports to test and evaluate new technologies for airport security. Hartsfield is the busiest airport in the world and you have had an initial glimpse at some of this. I do not ask for a judgment now, but could Hartsfield be one of those airports that you might consider that would be in that top 20 to test run, to test out some of your new technologies for airport security?

Mr. JACKSON. We are going to put in place—a competitive grant program is going to be the vehicle by which we run these pilot programs and it will be very important for the large airports with the significant volume and the complexity of issues to be active participants in that grant program so we can deploy the high end solutions to make sure that we have tested them rigorously. I can just say without having announced the details of the program that we would be delighted to work with Hartsfield should they wish to apply for some of this pilot experience with us.

Senator CLELAND. I am sure Ben DeCosta and his staff have heard that. And with that, I think it would be a good idea to take about a 5-minute break and go to our second panel.

Mr. Jackson, thank you very much for your willingness to come and be with us today. This is the first aviation security hearing after passage of the aviation security bill and I am sure it will not be the last. Thank you for working with us.

I will say, just a commendation to those incredible people from Norm Mineta on down, as soon as the events of September 11 unfolded, the United States Department of Transportation and the FAA and the pilots of America, the air traffic control people, everybody involved in the aviation system did an amazing thing. Within 2 hours, they landed every aircraft in America safely. And who knows but what that might have prevented another mishap and have saved lives. So that was an incredible achievement and yet our task is even greater now, to secure the nation's airways so that our public can get back to flying again, which is what we all want to do.

Thank you, Mr. Jackson, for being with us.

Mr. JACKSON. Thank you very much.

Senator CLELAND. We will take a 5-minute break.

[Recess.]

Senator CLELAND. We will come back to order here. We will have our panelists take their seats, if you will. Thank you very much for coming, gentlemen.

We would like to lead off today with Mr. Ben DeCosta, who is on the front lines of aviation security here, running the busiest airport in the world. We are delighted to have him here today and some members of his security team, Colonel Brooks and Richard Duncan.

Mr. DeCosta, would you like to share with us some thoughts?

STATEMENT OF BENJAMIN R. DECOSTA, AVIATION GENERAL MANAGER, HARTSFIELD ATLANTA INTERNATIONAL AIRPORT

Mr. DECOSTA. Good morning, and thank you. It is a pleasure being here with you. We very much appreciate the focus and emphasis that you have given airport security.

As you mentioned in your opening remarks, Hartsfield is the largest economic generator in the southeast and the busiest airport in the entire world. I appreciate this opportunity to participate in this hearing on these matters of immense importance.

I have abbreviated my testimony for the purposes of this hearing and would like to request that the entire testimony be submitted for the record.

Senator CLELAND. No objection, so ordered.

Mr. DECOSTA. Few topics are as important to our Nation right now as airport security. In the aftermath of September 11, it is essential that we do all we can to bolster the security at our nation's airports and restore the confidence of the traveling public.

As the world's busiest airport, more than 80 million passengers annually pass through our gates. We want to do everything we can to ensure the safety of those passengers and visitors.

Security has always been and will continue to be a top priority at Hartsfield. In 1999, the Atlanta City Council encoded Federal security regulations into our city ordinances which has allowed Hartsfield to assess fines and other penalties against companies and individuals who violate our security rules.

For more than 2 years, Hartsfield has given employees financial incentives also to challenge workers in secured areas who lack proper identification and our security checkpoints are among the world's most effective with some of the lowest error rates in the nation, despite the fact that we screen tens of millions of people every year. Security, therefore, has always been of high importance to us at Hartsfield.

In the wake of September 11, we have redoubled our efforts to make the airport secure and also to reassure the traveling public. We have fully implemented each and every Federal security regulation and measure and bolstered them with security reinforcements from the Atlanta Police Department, from Federal law enforcement agencies and from neighboring municipalities such as Clayton County.

We have welcomed the deployment of the Georgia Sky Guards to help monitor security screening operations. Here in the audience today is Colonel Bill Thomas, who is the leader of the National Guard at Hartsfield. Currently, National Guardsmen are employed at checkpoints and on the concourses. Their presence enhances the confidence of the traveling public.

We also welcome enactment of the Aviation and Transportation Security Act and the subsequent creation of a Transportation Security Agency. We are confident those measures will further enhance our security efforts and we are hopeful they will be effective in securing additional funding for airport security.

In your opening remarks, and I have heard you say that September 11 has really hurt the airlines and the aviation industry. I would just like to remind everyone that the airports have also been hurt with increased expenses and lowering of our revenues.

As you know, funding for enhanced security is of utmost importance. Hartsfield has devoted tremendous resources to fully implement the new security measures, even as revenues have fallen due to reduced air travel. We are allocating more than one million dollars per month on increased law enforcement alone. Unlike air car-

riers, airports have not received Federal funding to offset the increased costs of doing business in a post-September 11 world. We need your help to ensure that airports receive funds earmarked specifically for enhanced security. In the past, security projects have had to compete for funds with other airport improvement projects. We would like to see airport funding remain at current levels while Congress creates a separate program to fund aviation security improvements.

Airports are the major hubs of our nation's transportation system and it is essential that we invest in security of those facilities and the safety of those who visit them.

The Aviation, Transportation and Security Act, combined with the necessary funding, will make tremendous in-roads in bolstering airport security. The Act, however, contains deadlines that the Transportation Security Agency, air carriers and airports may find difficult to meet. Some say the deadlines are impossible. Most notable are the requirements to screen 100 percent of checked bags within 60 days and the deployment of explosive detection systems within 1 year. Obtaining the necessary personnel to meet the 60-day requirement could be very, very problemmatic. There are also concerns about the physical requirements—that means the facilities, terminal facilities—and the lack of facilities to accomplish the deployment of these explosive detection devices. My staff anticipates that we would need somewhere north of 60 such machines to satisfy the peak demands at Hartsfield. Our engineers and planners are reviewing space requirements, facility designs and other issues to support the installation of new equipment as it becomes available.

We applaud provisions of the Act that will add $2.50 to every flight to pay for security. Again, we hope Congress will restrict the use of those funds to airport security requirements. As you know, we currently collect funds to support Federal inspections at our airports. However, we have faced a challenge of low Federal staffing levels during peak international travel times. This is true of both INS and Customs staffing. We cannot afford to face those obstacles when it comes to the federalization of checkpoint screening.

Hopefully, the new funds will provide for sufficient numbers of Federal screeners to ensure that the traveling public will spend less than 10 minutes in line at any security screening point. Again, echoing what Mr. Jackson said, world class security and world class customer service. Our customers are demanding faster, better and more secure services at ticket counters, security screening areas and other areas of the airport. We hope that the Transportation Security Agency will embrace customer service as one of its security cornerstones. It is obvious they will, since Secretary Mineta has said so.

Finally, Section 114 of the Act must be expanded to punish individuals who violate security rules and regulations at airports. Currently, the Act increases penalties for individuals who assault or intimidate security personnel at airports or on aircraft; however, there are no Federal penalties imposed on individuals who commit other serious security breaches. A recent breach in our security apparatus, for instance, revealed that there are no Federal penalties for such breaches of security.

Airports are being asked to bolster security and taxpayers and travelers are being asked to spend billions for additional security measures to ensure the safety at our airports and yet, flagrant, willful violations of those security measures apparently are not against the law. We at Hartsfield believe that they ought to be. We agree with you, Senator Congress must enact tough Federal penalties that will deter individuals from breaching airport security. Such breaches are a threat to the safety of thousands of passengers and visitors. They destroy public confidence in security systems taxpayers and travelers have spent billions of dollars to erect. Security breaches inconvenience thousands while costing millions of dollars in flight delays and lost productivity. They ought to be against the law and there ought to be strong penalties for those who violate airport security.

I would like to thank you again for allowing Hartsfield to join you in this important hearing. We are proud of our efforts to increase security while maintaining our ability to provide quality customer service. We appreciate your focus, Senator Cleland, and that of the Committee on this important topic and for your efforts to help enhance security at our nation's airports. We look forward to working with the Committee and the Federal agencies to help reestablish the public's trust and confidence in safe and efficient air travel.

[The prepared statement of Mr. DeCosta follows:]

PREPARED STATEMENT OF BENJAMIN R. DECOSTA, AVIATION GENERAL MANAGER, HARTSFIELD ATLANTA INTERNATIONAL AIRPORT

Good Morning, I am Ben DeCosta, the Aviation General Manager for Hartsfield Atlanta International Airport. I would like; to thank Senator Cleland and the Senate Committee on Commerce, Science, and Transportation for holding this hearing to shed light on this critical issue. Few topics are as important to our Nation right now as airport security. In the aftermath of September 11, it is essential that we do all we can to bolster the security of our nation's airports and to restore the confidence of the traveling public. As the world's busiest airport, more than 80 million passengers annually pass through our gates. We want to do everything we can to ensure the safety of those passengers and visitors.

Security has always been a priority at Hartsfield, and we have been very proactive in the implementation and enforcement of aviation security rules. In October 1999, we implemented two programs aimed at improving employee security awareness and compliance with rules. Our first program focused on security compliance and enforcement, while the other program focused on rewarding individuals for actively participating in our security program. We asked the Atlanta City Council to integrate into the City's Aviation Code the Federal Aviation Regulation's individual responsibility provisions. This ordinance allows me to assess monetary and other penalties against companies and individuals for violating security rules. As a result of this ordinance, we have seen a much higher level of compliance with security rules by airport employees.

Additionally, we instituted the Hartsfield Harry Program to reward employees for taking an active role in airport security. Hartsfield Harry encourages airport and airline employees to challenge personnel found on the ramp without proper identification. Our security staff conducts tests throughout the airport to monitor compliance with security regulations. If an employee challenges "Harry,"—a security staffer who has entered a secured area without wearing proper identification—that alert employee receives a $25 check and becomes eligible for a quarterly drawing that awards $500 to the winner. Our compliance and enforcement program and Hartsfield Harry Program are two examples of our commitment to creating a safe and secure environment for the traveling public and airport employees.

In the wake of the September 11, 2001 tragedy, we have reviewed our security posture and have fully implemented all necessary security measures to further enhance our security program. On September 11, we increased our law enforcement support by 300 percent, thanks to the tremendous support received from the city

of Atlanta Police Department, Federal law enforcement agencies and other local municipalities. In fact, the Clayton County Police Department is actively patrolling the outer perimeter of the airport. The mutual aid received from these agencies allowed us to quickly evacuate the airport, search the terminal building and prepare the airport for the reception of passengers on September 13, 2001. We also welcomed the deployment of the Georgia Sky Guards to assist in the monitoring of security screening operations. We were pleased when Guardsmen were given authority to support our law enforcement efforts in other areas of the airport, such as on the concourses.

The airport community has responded positively to our increased security awareness through its involvement in the Airport Security Consortium. Our consortium, under the leadership and direction of our Aviation Security Manager, Richard Duncan, is meeting regularly to review security directives and assess their impact on airport operations. The consortium motto is "Security is Everybody's Business;" therefore, it insists on the complete involvement of all partners while implementing security measures. The consortium developed plans for revalidating security badges, searching incoming vehicles and reducing the number of access portals while maintaining our ability to provide quality customer services to our passengers and employees. We have devoted a tremendous amount of resources to ensure the full implementation of the additional security requirements, even though our revenues have decreased as a result of the reduced air travel. We are spending more than a million dollars per month on increased law enforcement coverage. Unlike the air carriers, airports have not received Federal funding to offset the increased cost of doing business in a post September 11th environment. We need your help to ensure that airports receive access to funds above the usual entitlement levels. If we were forced to use entitlement funds for special security needs, we would be forced to cut improvements needed elsewhere. We need a special security grant to offset the increased cost of security and unfunded mandates.

We welcomed the enactment of the Aviation Security and Transportation Act and the subsequent creation of the Transportation Security Agency. We hope that the agency will streamline the process for airports to receive Federal funds for airport security improvements. In the past, security projects have competed with other highly visible and important airport improvement projects for the same pot of money. I would like to see the airport entitlements remain at the current level while Congress creates a similar entitlement program that would fund aviation security improvements. Since airports serve as the linchpin of our national transportation and commerce system, we must ensure that our Nation contributes to the cost of creating and maintaining a secure and safe environment.

Although the Act is good in itself; it contains some extremely ambitious deadlines for the Transportation Security Agency, air carriers and airports. Most notable are the requirements to screen 100 percent of checked bags within 60 days and the deployment of explosive detection systems within 1 year. I'm not sure if the agency or air carriers can obtain the necessary personnel resources to meet the 60-day requirement. I have heard some discussions concerning the use of National Guard soldiers to fill the gap while the agency hires employees and acquires equipment to meet these challenges. Additionally, I'm concerned about the physical requirements and the lack of facilities to accomplish these objectives. After a recent briefing from the Federal Aviation Administration's new equipment integration team, my staff anticipates we would need 40 or more explosive detection system machines to satisfy our peak demands. Our engineers and planners are reviewing space requirements, facilities designs and other issues to support the installation of the new equipment: as it becomes available.

The 60-day requirement for 100-percent bag screening will be difficult, if not impossible, to meet at this airport. Positive bag matches, hand searches and the use of K-9 teams are not real alternatives for solving this challenging task. We simply don't have the space necessary for positive bag matching and hand searches of this magnitude. Additionally, our K-9 teams must be available to respond to law enforcement concerns.

We applaud the provisions of the Act that will add $2.50 to flight segments to pay for security. We also hope that Congress will restrict the use of these funds to airport security requirements only. As you know, we currently collect funds to support Federal inspections stations; however, we have faced the challenge of low Federal staff levels during peak international travel periods. We cannot afford that kind of challenge with security screeners; it is critical that we have sufficient staffing for screening stations. We hope that the collected funds would provide significant Federal screeners to ensure that the traveling public will spend less than 5 minutes in line at a security screening area. Our customers are demanding faster, better and more secure services at ticket counters, security screening areas and other areas of

the airport. We hope that the Transportation Security Agency would embrace customer service as one of its policy cornerstones.

Section 114 of the Act must be expanded to punish individuals who violate security rules and regulations at airports. Currently, the Act increases penalties for individuals who assault or intimidate personnel performing security duties at airports. However, there are no Federal provisions to punish individuals who commit other serious security violations. When a football fan bolted down an escalator recently without subjecting himself to the screening process, we had to evacuate and re-screen all passengers at the airport. This process took over 3 hours, interrupted the travel plans of tens of thousands of customers and cost the air transportation system millions of dollars. After finding the individual, it was very disheartening to learn that he had not violated a Federal law. Airport operators must have the support and backing of the Federal penal system to ensure that individuals are punished for failing to comply with Federal security rules. We must have security deterrence that discourages individual violators. We believe that a Federal law against airport security infractions would send the right message to the general public.

Finally, Hartsfield Atlanta International Airport would like to be one of the 20 airports selected to test and evaluate new and emerging technology, including biometrics, for providing access control and other security protections for secured areas of airports. If the technology works at the world's busiest airport, it will work at other airports, too.

In closing, I would like to thank the committee for choosing Atlanta as the site for this hearing. We are proud of our efforts to increase security while maintaining our ability to provide quality customer service to our customers. We have devoted the necessary resources to implement the new security directives at considerable expense of the city of Atlanta. We believe that airports must get some help from Federal agencies to continue the same level of support for an undetermined period of time. Furthermore, we will continue to work with all entities to help re-gain the public's trust in the aviation industry as the Transportation Security Agency assumes its role at this airport.

Thank you again for allowing Hartsfield to join you in this important hearing. We are proud of our efforts to increase security while maintaining our ability to provide quality customer service. We appreciate your focus, Sen. Cleland, and that of the committee on this important topic, and for your efforts to help enhance the security of our nation's airports. And we look forward to working with the committee and Federal regulatory agencies to help re-establish the public's trust and confidence in safe and efficient air travel.

Senator CLELAND. Thank you very much, Mr. DeCosta, you are doing a great job with a real world class mission here.

May I just say thank you for your support of legislation that I will introduce this afternoon when I get back to Washington to make it a Federal crime to deliberately breach security at an American airport. As I have said, I was out there on the tarmac and went through that experience and believe me, those of us on the aircraft would have had the penalty a little bit tougher. But I think that is the right way to go and thank you for your support.

May I say that the $2.50 passed in the aviation security law will go to buttressing our aviation security. It is fenced off and it will go to that purpose. Additionally there were other monies, about $1.5 billion, in the aviation security bill that will go to airports for your enhanced security and we just finished with the Defense appropriations bill Friday night about midnight and there is another $200 million there for airport security.

So there is going to be some monies coming down the pipe. The $1.5 billion I understand is on a competitive grant basis. So Mr. Jackson here invited you to apply for some of that.

Mr. DECOSTA. We certainly will and intend to.

Senator CLELAND. You and your staff will be aware of that.

May I just recognize Mr. Robert Hightower, the Georgia Commissioner of Public Safety, who is with us today and the Governor's designee in leading homeland security here in Georgia, and Gary

McConnell who is no stranger to challenges and difficult situations and disasters and attacks, mostly in terms of nature's revenge on us in terms of tornadoes and hurricanes and so forth—Gary McConnel, head of GEMA, we are glad to be with all of you.

Let me just go back, Mr. DeCosta, to that incident on November 6 when an individual caused a mass evacuation at Hartsfield when he intentionally breached airport security. Hartsfield correctly followed FAA procedure in temporarily halting incoming and outgoing air traffic. The incident did cause long delays and flight cancellations.

Can you tell me what, if anything, do you believe can be done to ensure that a similar breach does not happen in the future?

Mr. DECOSTA. Well, we have taken many steps. We had many lessons learned that day and have taken procedural, process steps, management steps to ensure that it does not happen again. We have employed some technology also. The public has heard us use the word Code Orange. We have strengthened our Code Orange procedures to ensure that it is far less likely that it would ever happen again.

As I said to the Airport Consortium, which is a group made up of the airlines, my own staff, the FAA and other tenants, that our goal, our objective is to make sure that that never happens again at Hartsfield. It is a tall order. Under the zero defect, zero tolerance policy where any breach could result in evacuation of the airport, we are taking every step to avoid that eventuality. What people do not realize is that those thousands of people who had to be evacuated from the airport were themselves, at least those who were frail, were put in harm's way by what we had to do.

Senator CLELAND. Thank you very much. And I certainly hope that the implementation of the aviation security bill and the increased penalty, which I hope to get through the Congress, will certainly help in that regard. Thank you very much.

Mr. John Selvaggio, Senior Vice President of Airport Customer Service with Delta, is here today. Thank you very much, John, for representing Delta. We would like to hear from you.

STATEMENT OF JOHN SELVAGGIO, SENIOR VICE PRESIDENT, AIRPORT CUSTOMER SERVICE, DELTA AIR LINES, INC.

Mr. SELVAGGIO. Senator Cleleand, thank you for this opportunity to appear today before the Committee to discuss aviation security. I am John Selvaggio, Senior Vice President of Airport Customer Service. My responsibilities include customer service functions at Delta's 163 airports worldwide and related security functions.

We are delighted that the Committee is holding this hearing, especially here in Atlanta, the home of Delta Air Lines and the site of Hartsfield Atlanta International, the world's busiest airport. We are also proud of the role you played, Senator Cleland, in sponsoring and passing the most comprehensive aviation security legislation in our nation's history. This landmark Act will build on the many comprehensive security programs established after the September 11th tragedy. It centers, appropriately, on a Federal, unified system. The Federal Government and the aviation industry have an enormous challenge in implementing the new law, but we are confident that we can deliver a safer and more secure system.

The Act transfers all security functions and activities to the Federal Government under the new Transportation Security Administration. We wholeheartedly support this change and Delta will work cooperatively to hand over these responsibilities, including passenger and bag screening to the Federal Government.

Senator Cleland, we are pleased to see your proposed legislation to make willful violations of airport security a Federal criminal offense. Secretary Mineta has stated that we must have zero tolerance of security breaches and we agree. Your legislation addresses a void in our criminal statutes and will prevent future violations of airport security, especially of the kind that crippled Atlanta Hartsfield a few weeks ago.

The American public and the Congress are demanding to know what measures are being taken to ensure that aviation security is increased. I am pleased to report to you today much has been done and there is a lot more to come.

Senator Cleland, since September 11, the U.S. aviation industry has worked assiduously with the Federal Government to undertake the following:

- Carrying Federal air marshals (FAM's) on an increased number of flights.
- Fortified cockpot doors.
- Conducting random physical searches of airline and airport personnel.
- Increasing airline staff to oversee security in airports.
- Conducting random physical searches and hand wand or pat down passengers at security checkpoints and boarding gates.
- Restricting carry-on baggage to one checked bag and one personal item for all flights.
- Cooperating with various governmental agencies in sharing passenger information.
- Comprehensive searches.
- Using advanced technology, (AT) and explosive detection system technology (EDS) extensively which provide comprehensive explosive detection, in many of the country's largest airports.
- Expanded searching of both checked and carry-on luggage.
- Conducting extensive random screening of all checked and carry-on luggage.

These steps have dramatically improved our industry's security and these measures have, in our view, helped restore public confidence in our system. However, with the passage of the Aviation and Transportation Security Act, additional steps will be taken to further enhance aviation security.

As the Federal Government moves to implement the new security program, we must keep the customer in mind. This means refraining from constructing a security system that is so cumbersome and onerous that the traveling public begins to see air travel as a burden, rather than as a convenience. To this end, we are fully supportive of working with the government to develop a Trusted Passenger Program, which with laser-like precision, will focus additional security measures on those that warrant it most, while minimizing inconvenience for the majority of passengers who are not perceived to be a threat.

Our customers at Hartsfield should not have to wait in line for hours to pass through a security checkpoint. We are pleased to see that Secretary Mineta is planning to establish customer performance standards. We applaud Secretary Mineta's statement that his goal in passenger screening is "No weapon, no waiting." The Secretary stated,

> "We will strive to develop a screening process that prohibits weapons or other banned materials in airport sterile zones without requiring a wait of longer than 10 minutes at any security checkpoint for passsengers using U.S. airports."

The new system must focus more on people and less on things. We need to be smarter in processing passengers and baggage and learn from the screening programs currently employed by the Customs Service and INS. We must meet that goal in order to retain a vibrant, stable and customer-focused air transportation system.

Senator, we face a national challenge, the likes of which we have not seen in our lifetime. Like the generations before us that made this country great by making it safe and secure, I know we are up to this challenge.

Again, thank you for the opportunity to share Delta's testimony with this Committee. I would be glad to answer any questions you might have.

[The prepared statement of Mr. Selvaggio follows:]

PREPARED STATEMENT OF JOHN SELVAGGIO, SENIOR VICE PRESIDENT, AIRPORT CUSTOMER SERVICE, DELTA AIR LINES, INC.

Senator Cleland, thank you for this, opportunity to appear today before the Committee to discuss aviation security. We are delighted that the Committee is holding this hearing, especially here in Atlanta, the home of Delta Air Lines and the site of Hartsfield Atlanta International, the world's busiest airport.

We are also proud of the role you played, Senator Cleland, in sponsoring and passing the most comprehensive aviation security legislation in our nation's history. This landmark Act will build on the many comprehensive security programs established after the September 11 tragedy. It centers, appropriately, on a federally unified system. The Federal Government and the aviation industry have an enormous challenge in implementing the new law, but we are confident that we can deliver a safer and more secure system.

The Act transfers all security functions and activities to the Federal Government under the new Transportation Security Agency. We wholeheartedly support this change and Delta will work cooperatively to hand over these responsibilities, including passenger and bag screening, to the Federal Government.

Senator Cleland, were pleased to see your proposed legislation to make willful violations of airport security a Federal criminal offense. Secretary Mineta has stated that we must have zero tolerance of security breaches. We agree. Your legislation addresses a void in our criminal statutes and will prevent future violations of airport security, especially the kind that crippled Atlanta Hartsfield a few weeks ago.

The American public and the Congress are demanding to know what measures are being taken to ensure that aviation security is increased. I am pleased to report to you today much has been done and there is a lot more to come.

Senator Cleland, since September 11, the U.S. aviation industry has worked assiduously with the Federal Government to undertake the following:

- Carrying Federal Air Marshals (FAM's) on an increased number of flights
- Fortifying cockpit doors
- Conducting random physical searches of airline and airport personnel
- Increasing airline staff to oversee security in airports
- Conducting random physical searches and hand wand pat downs of passengers at security checkpoints and boarding gates
- Restricting carry-on baggage to one checked bag and one personal item for all flights
- Cooperating with various governmental agencies in sharing passenger information

• Comprehensive aircraft searches
• Using advanced technology (AT) and explosive detection system technology (EDS) extensively, which provide comprehensive explosive detection, in many of the country's largest airports
• Expanded searching of both checked and carry on baggage
• Conducting extensive random screening of all checked and carry-on luggage

With the passage of the Aviation and Transportation Security Act, additional steps will be taken to further enhance aviation security.

As the Federal Government moves to implement the new security program, we must keep the customer in mind as we move forward. This means refraining from constructing a security system that is so cumbersome and onerous that the traveling public begins to see air travel as a burden, rather than a convenience. To this end, we are fully supportive of working with the government to develop Trusted Passenger Programs which, with laser-like precision, will focus additional security measures on those that warrant it most, while minimizing inconvenience for the majority of passengers who are not perceived to be a threat. Our customers at Hartsfield should not have to wait in line for hours to pass through a security checkpoint. We are pleased to see that Secretary Mineta is planning to establish customer performance standards.

The new system must focus more on people and less on things. We need to be smarter in processing passengers and baggage and learn from the programs currently employed by the Customs Service and INS.

We applaud Secretary Mineta's statement that his goal in passenger screening is "No weapons, no waiting." The Secretary stated,

> "We will strive to develop a screening process that prohibits weapons or other banned materials in airport sterile zones without requiring a wait of longer than 10 minutes at any security checkpoint for passengers using U.S. airports."

We must meet that goal in order to retain a vibrant, stable and customer-focused air transport system.

Senator, we face a national challenge the likes of which we have not seen in our lifetime. Like the generations before us that made this country great by making it safe and secure, I know we are up to this challenge.

Again, thank you for the opportunity to share Delta's testimony with this Committee. I would be glad to answer any questions you might have.

Senator CLELAND. Thank you very much, Mr. Selvaggio.

Do you feel that air travel is safer and more secure today than it was September 10?

Mr. SELVAGGIO. I think to be perhaps a bit redundant, we have enacted so many new layers in the fabric of security, that it is vastly safer today than it was on September 10.

Mr. Jackson mentioned several of the things we did. In my testimony, I also did. But I would like to point out that we have really put a lot of attention on the people. We have ensured that all Delta people and the contractors who service us on the ramp are inspected. We have revalidated all of our employee identification badges, including comparing all the names with the FBI watch list. We mentioned that we fortified cockpit doors on our airplanes. In addition to that, Delta has also introduced a prototype of a video system on board the airplane which enables the crew to see what is going on inside the aircraft.

But essentially, our mission is that, you know, we want to ensure that the passenger screening process scrutinizes those passengers who we know the least about and we try to direct our efforts there.

Senator CLELAND. Do you think that the federalization of our system, the unified system, with its intelligence-gathering capability and intelligence-sharing capability will indeed be able to do exactly what you suggest, focus more on passengers rather than on things?

Mr. SELVAGGIO. We think that is a very noble objective. We have got great technology today that can help us take a passenger from

the time they book—you mentioned an example of a passenger boarding an aircraft in Sweden, Stockholm I think, and having the United States get a heads up while they are en route. We believe that we can start that process when a passenger books a reservation. We think that we have the technological capabilities to determine if that is a trusted passenger or not. We know that the resources available include the FBI watch list as well as other law enforcement data bases as well as Federal Government and airline data bases, and we think that if you can combine the data bases and the wealth of information we have with the technology we have, we think that we can go a long way to improving security before the customer or the passenger even gets to the airport.

Senator CLELAND. How do you think you are going to fare with the challenge of checking all checked baggage that goes in the belly of an aircraft within the next year, having December 31 as that deadline? How do you think you will be able to meet that?

Mr. SELVAGGIO. We believe it is going to be extremely challenging and that the screening process will have to include some element of increasing the computer assisted profiling system that we have today. We plan to use every means available from the sniff dogs to hand searching bags as well as the EDS machines that are available. However, as Mr. DeCosta mentioned at the Atlanta airport, for example, we are dreadfully short of the number of machines it would take. We are also very mindful of the fact that we do not want to make the system so burdensome for the customer that the customer will look for other means of travel.

We are very aware that a good portion of our business travel here in Atlanta uses aircraft in lieu of driving. So if the cumbersome—if it becomes too cumbersome to check in an airport, we are concerned that people will drive. So we have to use every ability, every means we have to enhance this process and try to get that 10-minute check-in delay to be the maximum we can live with.

Senator CLELAND. Thank you very much.

Mr. Tom Kalil, Senior Vice President of Customer Service is with us today representing AirTran and we are just delighted to have you here, Mr. Kalil. Some words, please.

STATEMENT OF THOMAS KALIL, SENIOR VICE PRESIDENT, CUSTOMER SERVICE, AIRTRAN AIRWAYS, INC.

Mr. KALIL. Thank you very much, Senator Cleland. I appreciate the opportunity to appear at this very important hearing.

As a veteran of some 42 years of service in the airline industry, I want to thank you, Senator, on behalf of AirTran Airways, for your important work on the Aviation Subcommittee. We appreciate your tireless efforts to ensure the safety of our national air transportation system and we thank you for conducting this important hearing today here in Atlanta. I also would like to thank Secretary Jackson for his leadership on security and so m any other key issues affecting transportation.

Senator, AirTran Airways is the second largest carrier at Hartsfield Atlanta International Airport. We flew more than 7.5 million passengers last year and we are proud of the role of AirTran in providing affordable and efficient air service to the traveling public in 36 cities.

I am also pleased to report to you today that despite the unprecedented challenges since September 11, AirTran is well positioned to succeed. We are among the very few airlines which are actually bigger today than we were on September 10th. We have increased our capacity by about 5 percent because we believe we can succeed in bringing our service to markets where service has been curtailed or abandoned by other carriers. We are particularly focusing our growth in small- and medium-sized markets.

Our ability to succeed is largely the results of the sacrifice and hard work of our employees. Shortly after September 11, our pilots and mechanics, through a combination of pay reductions and work rule changes, voluntarily reduced payroll costs by almost 20 percent. Our corporate officers and other levels of management made similar sacrifices. That effort preserved our ability to survive and compete and it largely prevented mandatory layoffs. The compensation reduction for our pilots and mechanics has been restored, although pay cuts for corporate officers and management remain in place.

I should add, Senator, that your strong support and successful enactment of the Aviation Safety and Stabilization Act was essential. Without the funding and the expectation of loan guarantees, I can assure you that most major and regional carriers could have been in bankruptcy by now, and the national economy would be in genuine chaos.

However, we still have a way to go. Airlines will not regain their full passenger loads and levels of service until and unless the public has complete confidence in their safety and their convenience when they fly.

At AirTran Airways, the security and safety of our passengers has always been our No. 1 priority and we have redoubled those efforts since September 11th.

We are proud of the fact that AirTran Airways was the first carrier in the Nation to complete the installation of FAA-approved cockpit door protection systems. Those doors cannot be rammed in, pulled open, or otherwise breached by a passenger. In addition, AirTran will be offering voluntary self-defense training to our flight attendants to provide additional security for our passengers and staff in the aircraft cabin.

We are also proud that AirTran in Atlanta and thrutout our entire system fully trained all of our own employees in the security measures that were enacted after September 11, and we contract no employees to do that. The FAA has been very pleased with our results and have commended our personnel on a number of occasions.

As we have seen from the exhibits today, technology is an important component of security. We are reviewing a number of promising new options ranging from new explosive and weapons detection devices to biometric identification cards for airport personnel and crew. We hope that the new retina scanning and fingerprint identification systems can be deployed. Later this identification could be extended to passengers who volunteer for security background check in order to receive expedited security screening at airports.

Senator, at AirTran, we believe there are three pillars to good security. No. 1 is the requirement for highly professional personnel with the best possible training and supervision. No. 2 is the best and most reliable security equipment and facilities. No. 3 is a consistent, comprehensive and workable Federal security plan.

The heart and soul of the system is the quality and training of our people. No matter how good our equipment and procedures may be, they are only as good as the people who operate them.

Technology is vitally important, particularly because it makes the system faster. People were patient during the busy Thanksgiving travel period, but patience will wear thin over time. Reliable technology—particularly the increased automation of our systems—is mandatory if we are going to bring passengers back to flying.

We must keep in mind that our current security systems are operating on the basis of a 15 to 20 percent reduction in capacity imposed by most airlines. When those capacity reductions are restored, we must be able to safely accommodate the increased volume of passengers and bags without increasing security delays.

In all respects, we must have a consistent, national system. An FAA security inspector in Dallas or Denver must impose the same high standards as one in Miami or Myrtle Beach, because we are only as strong as our weakest link. Our general impression from pilots and crew members is that security practices are inconsistent from airport to airport.

Finally, Senator Cleland, I hope that Congress will revisit the issue of how to pay for this system. With the imposition of the new $2.50 security fee per flight segment, taxes and fees now comprise as much as 26 percent of the price of a ticket. This is as much as a 35 percent increase in the cost of ticket taxes to passengers. We know from our own experience that these marginal increases have a clear and negative impact on stimulating air travel.

Senator, that concludes my remarks and again, I thank you for the opportunity to appear at your hearing.

[The prepared statement of Mr. Kalil follows:]

PREPARED STATEMENT OF THOMAS KALIL, SENIOR VICE PRESIDENT, CUSTOMER SERVICE, AIRTRAN AIRWAYS, INC.

Senator Cleland, members of the commerce committee staff, and guests, I appreciate the opportunity to appear at this important hearing.

As a veteran of some 42 years of service in the airline industry, I want to thank you, Senator, on behalf of AirTran Airways for your important work on the Aviation Subcommittee. We appreciate your tireless efforts to ensure the safety of our national air transportation system, and we thank you for conducting this hearing in Atlanta. I also would like to thank Secretary Jackson for his leadership on security and so many other key issues affecting transportation.

Senator, AirTran Airways is the second-largest carrier at Hartsfield Atlanta International Airport. We flew more than 7.5 million passengers last year, and we are proud of the role of AirTran in providing affordable and efficient air service to the traveling public from 36 cities.

I am pleased to report to you that, despite the unprecedented challenges since September 11, AirTran is well positioned to succeed. We are among the very few airlines that are actually bigger today than on September 10. We have increased our capacity by about 5 percent because we believe we can succeed in bringing our service to markets where service has been abandoned or curtailed by other carriers. We particularly are focusing our growth in small and medium sized markets.

Our ability to succeed is largely the result of the sacrifice and hard work of our employees. Shortly after September 11, our pilots and mechanics, through a combination of pay reductions and work rule changes, voluntarily reduced payroll costs by almost 20 percent. Our corporate officers and other levels of management made

similar sacrifices. That effort preserved our ability to survive and compete, and it largely prevented mandatory lay-offs. The compensation reductions for pilots and mechanics have been restored, although pay cuts for corporate officers and management remain in place.

I should add, Senator, that your strong support and the successful enactment of the aviation safety and stabilization act was essential. Without the funding and expectation of loan guarantees, I can assure you that most major and regional carriers could have been in bankruptcy by now, and our national economy would be in genuine chaos.

However, we still have a way to go. Airlines will not regain their full passenger loads and levels of service until and unless the public has complete confidence in their safety and their convenience when they fly.

At AirTran Airways, the security and safety of our passengers has always been our No. 1 priority, and we have redoubled those efforts since the tragedies of September 11.

We are proud of the fact that AirTran Airways was the first carrier in the Nation to complete the installation of FAA-approved cockpit door protection systems. Those doors cannot be rammed in, pulled open, or otherwise breached by a passenger. In addition, AirTran will be offering voluntary self-defense training to our flight attendants to provide additional security for our passengers and staff in the aircraft cabin.

We also are proud that AirTran was the first carrier in Atlanta to fully train our own personnel in the new FAA security procedures. We hire no contract employees to conduct security checks—all of those personnel are AirTran employees. The FAA has been very pleased with our results and commended our personnel on a number of occasions.

As we have seen from the exhibits today, technology is an important component of security. We are reviewing a number of promising new options, ranging from new explosive and weapons detection devices to biometric identification cards for airport personnel and crew. We hope that the new retina scanning and fingerprint identification systems can be deployed. Later, this identification could be extended to passengers who volunteer for a security background check in order to receive expedited security screening at the airport.

Senator, at AirTran we believe there are three pillars to good security. No. 1 is the requirement for highly professional personnel with the best possible training and supervision. No. 2 is the best and most reliable security equipment and facilities. No. 3 is a consistent, comprehensive, and workable Federal security plan.

The heart and soul of the system is the quality and training of our people. No matter how good our equipment and procedures may be, they are only as good as the people who operate them.

Technology is vitally important, particularly because it makes the system work faster. People were patient during the busy Thanksgiving travel period, but patience will wear thin over time. Reliable technology—particularly the increased automation of our systems—is mandatory if we are to bring all of our passengers back to flying.

We must keep in mind that our current security systems are operating on the basis of the 15 to 20 percent reductions in capacity imposed by most airlines. When those capacity reductions are restored, we must be able to safely accommodate the increased volume of passengers and bags without increasing security delays.

In all respects, we must have a consistent, national system. An FAA security supervisor in Dallas or Denver must impose the same high standards as one in Miami or Myrtle Beach because we are only as strong as our weakest link. Our general impression from our pilots and crews is that security practices are inconsistent from airport to airport.

Finally, Senator Cleland, I hope that the Congress will revisit the issue of how to pay for this system. With the imposition of the new $2.50 security fee per flight segment, taxes and fees now comprise as much as 26 percent of the price of a ticket. That is as much as a 35 percent increase in the cost of ticket taxes to passengers. We know from our own experience that these marginal increases have a clear and negative impact on stimulating air travel.

Senator, that concludes my remarks, and again, I thank you for this opportunity and for calling this hearing.

Senator CLELAND. Well, thank you, Mr. Kalil, I appreciate that statement, and you are right, we have to be sensitive to the ticket price. That is something that we have to always pay attention to.

Let me just ask you a question: How do you think AirTran is going to be able to handle the requirement of checking all checked baggage by December 31 of next year, for explosive devices?

Mr. KALIL. We will very aggressively pursue the acquisition of whatever technology we need, training of our people, and we feel extremely confident that while it is going to be difficult, it is going to be costly, that we will be in a position to implement at the time it is required to do so.

Senator CLELAND. OK, thank you very much for that commitment.

Now we move to the technology of dealing with the challenge of increased world class security, world class customer service. Dr. Bevan, is it? Tom Bevan is Director, Georgia Tech Center for Response Technologies—and if we ever needed a technological response to help out our country, it is right now, Doctor. He is with Georgia Tech, the Georgia Tech Research Institute. Thank you for being here with us, we are glad to hear from you.

STATEMENT OF DR. THOMAS BEVAN, DIRECTOR, GEORGIA INSTITUTE OF TECHNOLOGY

Dr. BEVAN. Thank you for inviting me to participate in this hearing. I want to especially commend you, Senator Cleland, for your many statements regarding issues pertaining to terrorist threats to our country and for organizing this hearing.

I would like to summarize my prepared remarks and have the text incorporated into the record, if I could.

About 3 years ago, with help from yourself, the Georgia delegation and the U.S. Marine Corps, Georgia Tech started a center to deal with weapons of mass destruction to get technologies into the hands of first responders and others who were going to have to deal with those kinds of incidents. We did not know where the terrorists would strike or how, but the feeling was that the first responders were always going to be on the line and that was a good place to start.

In addition to working on technologies, we also tried to address policy and training issues so we have some experience there to fall back on, particularly the command and control issues and that arena.

So we started from the grassroots. We now have 50 regional partners and some of them are here today, including GEMA, the CDC and GMAG, the Georgia Mutual Aid Group. Last year, about a year ago today, we demonstrated six technologies that might be useful to deal with weapons of mass destruction incidents. By weapons of mass destruction, I also include high-explosive chem-bio weapons.

When 9/11 and the subsequent anthrax attacks occurred, we have broadened our initiative now to expand it to some other areas, first in aviation security and airport security, and I will show you some technologies that we picked out that we think might be useful there. We are also working with the CDC on two projects; one dealing with air intake to buildings, trying to protect first the CDC buildings and then other buildings, including commercial buildings. Some of the same techniques there also apply to protecting air intakes in airplanes and airports, which are potential targets.

And then we are also working with the CDC on using advanced technology to improve epidemiology so that it becomes near real time and of course that is important for aviation safety because in a biological weapons attack using an infectious agent that could create in an airport or an airplane, could create a big epidemiology problem that has to be solved quickly.

And then finally, we are looking at what basic research areas really need to be attended to—things like technology that can help us build better composites for aircraft doors and so forth.

Before I show you some of these technologies, I wanted to make a couple of points. One is the existence of these technologies, the technologies exist to help. And just as we found in the first responder situation, a lot of them have been overlooked by government funding agencies. They tend to not meet military specifications for what they want, but yet they are still quite useful. So there are technologies out there in existence. The other is that technology can be used to foster communications and cooperation between various organizations, particularly the information technologies.

But we need to do a better job right now of getting some of these technologies transitioned, out the doors of universities and not-for-profits where they have been developed typically with Federal money—to get them out the door and into the hands of users. Given the slowdown in the economy, there is not a lot of risk capital around to accelerate that process.

So that is the third point I would make, the government needs to perhaps step in and try to help facilitate tech transfer here.

So I will talk to you about four—these are representative technologies in four areas I will talk about. The first area is the sensor technology. One would like to sense very quickly chemical, biological, radiological, high-explosive materials. This technology really started—is about 12 years old, it has been sponsored by the State of Georgia for inspection of wash water off of chickens looking for salmonella infection. The idea is that the same sort of mechanisms might be useful for anthrax or other types of biologicals.

And then the other area is from the environmental industry. We have gotten very little money from military or other folks until last year. So the sensor we figure, the piece parts are about a hundred bucks as opposed to some sensors that might be used which are $100,000 and might need a Ph.D. to operate. This one is very simple. The piece parts are a laser, the same laser that is in your CD-Rom reader in your computer, it costs about ten bucks, on a one-piece part basis; a glass slide which has a chemically sensitive coating and the laser light goes through that slide; and then a readout device. This is a CCD readout device. Right now we are actually cannibalizing those from web cameras that we can buy for 40 bucks at Radio Shack. So the technology—it took us 12 years to get to make it simple, I should also hasten to say.

So the technology is there and what essentially happens is that this chemically sensitive coating can get exposed to a chemical or biological agent and when it does, there is a chemical reaction that occurs. That chemical reaction actually changes the speed of light through the wave guide, which is this glass slide here. When that occurs, we can sense that with a readout device. A light goes on

and you can tell not only what type of agent it is but also get an instantaneous readout of its concentration.

We think that technologies like this—and Georgia Tech is also developing some five other technologies which are more basic further down the road for implementation—technologies like this might be incorporated in an aircraft or in airports looking for these kind of agents. So that is the sensor arena.

In a couple of the exhibits here in the physical security arena, one of the things you would like to do is reinforce the doors of cockpits. The ideal material for that are composites, plastics, and we are looking into what we should be doing there, particularly for reinforced plastics.

One of the things you would like to do is you would like to have iron bars on the cockpit, reinforce the composites or the door with essentially bars of metal. The problem with that is they are too weighty, they are too heavy. So we have developed some materials here that are extruded that have almost the same properties, if you tried to puncture them or bend them, as solid bars, but they are honeycombed with cellular materials that brace each other and, therefore, make it very lightweight as well as very strong. So we are continuing to work in those kinds of materials and I have actually talked to some folks here in the airline industry that are interested in coming to work with us on that.

The next piece of technology is a filter that looks like it is full of jello. It is actually not jello, it is a substance called hydro-jells or sol-jells and these are polymers that are impregnated with water and other materials so that they can catch particulate matter, say anthrax-sized particulate matter. They also have some other nice properties in that they capture and hold chemicals, particularly volatile or organic chemicals. One of the strategies one might use if you are a terrorist and want to attack an air conditioning system, air intake, is to fill it full of volatile organics or cyanide that would clog up conventional carbon filters, which are the kinds that are in gas masks essentially. And then you follow that with, you know, nice things like nerve agents that would kill a lot of people. So essentially, the idea is you clog up the filters and then you get stuff through them that would hurt people.

This has some nice properties in that it captures volatile organics but it captures a lot of them. It has a lot of reserve and would help to address that type of attack.

So that is some of the physical security issues.

The other area is information technology and you had a hearing on Wednesday to talk a little bit about information technology. What we did with our first responders is we—they respond in the form of an organization called an incident command post at one of these chem-bio events. The case in New York City, they had some 24 of them, primarily because they had communications problems. You ideally would like to have one that coordinates everything. But what we did with them was we—it is now possible with wireless local area networks and wireless wide area networks to get communications from individual firemen, even those in the hot zone with chem-bio agents, to get communications to and from them using these portable devices. Right now, this one is actually communicating with a local area network hub which is out in the hall, so

I can get information to and from this Palm Pilot. It's essentially a standard Palm, this is all commercial off-the-shelf technology—a Palm Pilot type machine with a wireless card.

Now applications for airports and in airplanes are—we believe we could give these to security people to exchange information, not only collect information around the airports about potential threats, but also tell them—keep them informed throughout the airport in more than you could do just through a radio. So it's both a data collection method as well as giving orders out. You know, our friend that ran down the escalator the wrong way, well it made me a little angry because I was sitting in one of the 60 other airplanes with my 87-year-old mother and she was having a hard time. But the idea is that if that kind of event occurs, we can alert all the security people, get a description and try to get him before he gets off the train.

Senator CLELAND. Right.

Dr. BEVAN. This also contributes to the information fusion situation where you have data bases, and we have talked about some of those, of potential terrorists. We can also contribute data collected from airports and from the airplanes to those data bases to try to get early detection.

Senator CLELAND. Do you just want to summarize?

Dr. BEVAN. Yes.

Dr. BEVAN. There is just one other technology I wanted to talk about and that is training technology. We are going to have to train about 30,000 new Federal employees. There are web-based training technologies that could help that we have either used or pioneered over the years. And also a side benefit from that is you get uniformity across all of the population you are trying to train. A lot of that technology is available commercially. So that is yet the fourth category.

[The prepared statement of Dr. Bevan follows:]

PREPARED STATEMENT OF DR. THOMAS BEVAN, DIRECTOR, GEORGIA INSTITUTE OF TECHNOLOGY

Thank you for inviting me to participate in this hearing. I want to especially commend you, Senator Cleland, for your many statements regarding issues pertaining to terrorist threats to our country and for organizing this hearing on aviation and airport security. I also thank you for your longstanding support of Georgia Tech and our efforts to address the threat of terrorism and weapons of mass destruction.

About three years ago, Georgia Tech formed the Center for Emergency Response Technology, Instruction and Policy (CERTIP) in order to address the needs of first responders in coping with terrorist attacks involving weapons of mass destruction including chemical, biological, radiological, nuclear and high-explosive (CBRNE) agents. We started with first responder issues because, while it was unclear how terrorists would attack or how our governmental agencies would respond, it was certain that local first responders would have to bear the brunt of any attack.

Over the past three years CERTIP has successfully demonstrated innovative, affordable, near-term technologies for first responders with the help of over 50 regional and national partners, the US Marine Corps and the Georgia Congressional delegation. We work directly with first-responders to identify requirements and test prototypes for rapid feedback to the developers. Our list of partners feature the US Marine Corps Systems Command, US Marine Corps Warfighting Laboratory, National Guard Bureau, Centers for Disease Control, Georgia Mutual Aid Group, CBIRF, Georgia Emergency Management Agency, Grady Hospital, the Atlanta Fire Department and the National Institute of Urban Search and Rescue. In November 2000, during "Project Atlanta" we staged a chemical agent exercise on the Georgia Tech campus and successfully demonstrated many new technologies to deal with

such incidents. I will show you several of these today because they also apply to aviation and airport safety.

The events of September 11th 2001 revealed that the terrorists had the will to exploit weaknesses in our aviation security and the willingness to sacrifice their lives to use weapons of mass destruction in the form of high explosive jet fuel. Shortly after that date, Georgia Tech launched its Homeland Defense Initiative to expand the scope of the Center's activities beyond immediate first responder issues. We are continuing to identify technologies that can be fielded in the near-term but are also attempting to identify basic research areas that can provide solutions in the long-term. We are looking at how we can contribute to counter-terrorism in the areas of intelligence, law enforcement, emergency management, military support, firefighting/hazardous materials, medicine, environment and transportation. For example, we are now considering how to approach fusion of many disparate information databases for aviation safety and early detection of biological warfare attack, the latter with the CDC.

Which brings us to aviation and airport safety.

To summarize the threat: airports and airplanes provide potentially lucrative targets for terrorists, particularly those with the capabilities to use weapons of mass destruction. Airports and airplanes contain dense concentrations of people—an ideal target for weapons of mass destruction. Airports and airplanes are particularly lucrative for spreading biological warfare agents, especially contagious agents where large numbers of people can be exposed to contagious diseases. Finally, there are psychological impacts of attacking airports and airplanes because many people have the shared experience of spending time in these locations.

This morning, I want to make three points regarding aviation and airport safety. The first point is that technologies exist or can be developed to improve counterterrorism and emergency response in aviation safety. Technologies will not solve all of our problems—safety requires dedicated, competent, trained people and appropriate government policy which encourages cooperation. I will show you some examples of existing and emerging technology today.

Second, aviation counterterrorism and emergency response require a new kind and level of cooperation between many organizations at many levels of government and in the private and not-for-profit sectors. Government needs to set and enforce policies and create incentives, which will encourage cooperative planning, materiel standardization, joint training and joint emergency response. For example, one of the main tenets in our CERTIP effort has been to bring all of the organizations, military and civilian, together to plan how to work together in CBRNE emergency response. At the grass roots, those responsible to prevent and deal with CBRNE terrorist incidents cooperate in spite of unclear, ambiguous government policy and organization. As in other counterterrorism areas, there now needs to be a top-down examination of policy and organization to insure cooperation in aviation and airport safety. We also need to focus on training for command and control of diverse organizations.

Third, we must invent mechanisms to get state-of-the-art and future technologies out of universities and not-for-profits and into the hands of users. I am speaking of a technology transfer initiative with the scope of a Manhattan Project. Currently the government funds university and not-for profit research and it also does a good job of funding government laboratories and for-profit corporations in order to keep essential development and manufacturing capabilities available for national defense needs. But with business as usual it often takes nearly 20 years to get new technologies fielded. We should establish the capability to coordinate national research efforts on a much broader scale and to connect near-term successes with the users—military and civilian—as quickly as possible. Furthermore, agencies need appropriate levels of funding and discretion to fund and field promising research. Georgia Tech has acted as a catalyst to get many new technologies into the hands of users in record time so we know that barriers exist. University and not-for-profit consortia, centers of excellence and proper funding are needed to encourage the emergence of these technologies.

For the purposes of this session, I will categorize some key aviation/airport security technologies in to four areas: (1) Sensors for CBRNE agents, (2) Physical Security, (3) Information Technology for communications and data exchange and (4) Training.

(1) *Sensors* are needed to detect CBRNE agents which might be used to attack aviation, airports and passengers. While there are many sensor technologies under development, I want to show you one in particular. Opto-electronic interferometric sensor technologies have been under development by Georgia Tech for the environmental and food processing industries for about 12 years. The current technology provides the means to field an affordable, small, lightweight, low-power device that

can detect and identify agents rapidly at low concentrations. The current device consists of three components: a small low-power laser, a planar optical waveguide with chemically sensitive coatings and a CCD camera readout. The total cost of the components, even in low quantities, is less than $100. Light is provided by the laser, which is channeled through the waveguide. The waveguide has up to 75 individual interferometers. Each interferometer has two light channels, which are directed together or interfered, at the end of the waveguide to produce an interference pattern. One of these two channels is painted with a chemical, which reacts with the chemical of interest. When this occurs, the speed of light through that channel is changed and the interference pattern starts to shift, identifying the chemical and providing its concentration. Last year, Georgia Tech CERTIP demonstrated that this technology could detect and discriminate sarin chemical agent surrogates. This year we set out to detect biological agent surrogates but after the anthrax letters were discovered the US Marine Corps requested that we begin to demonstrate the ability to detect anthrax.

Other sensor technologies under development at Georgia Tech include the capability to field laboratory-grade instrumentation using very small components. Another sensor technology has already demonstrated the capability to detect cocaine in small quantities for the US Customs Service and could be tuned to other chemicals.

(2) *Technologies for physical security* include both hardware and software. For example, Georgia Tech is developing materials which could provide cockpit or airport doors, which are more resistant to penetration. These include composite materials, linear cellular alloy reinforcements and nano-fiber reinforced materials, which are even stronger and resist penetration. More advanced "shape-shifting" materials that swell in response to electrical or thermal energy, can seal doors in the doorway but provide rapid opening.

Georgia Tech CERTIP is also partnering with the CDC and Auburn University on the Air Intake Protection Program to develop sensors (the opto-electronic sensor, described above, is being used) and filtration systems to protect CDC buildings from attack. Obviously, the results of the Air Intake Protection Program could be used to protect commercial and private buildings, as well. Georgia Tech also has interest in developing materials to absorb cargo hold explosions and avoid penetration of vital systems in aircraft.

Off-the-shelf and developing software systems and techniques can analyze passenger information to look for suspicious patterns of behavior (assisted by realtime inputs from wireless information technology, see below). Another software technology provides the means for identifying potential terrorists involves face recognition. Face recognition technology can be enhanced with a model of the human visual system called GTVision. GTVision is an engineering model, which captures the state-of-the-art in our knowledge of human vision from the eyeball through the brain. It is recognized as a world-class model by the US and UK military and is used by the military to develop camouflage patterns and predict human visual performance. This model also functions as a pattern recognition algorithm that can be used to identify people through facial features or could be used for biometric recognition systems.

(3) *Information technology* is one of America's strengths and should be used to provide survivable, interoperable and convenient communications and data exchange. This was pointed out in recent hearings in which you participated.

In the aftermath of the 9/11 tragedy in New York City, the Internet was the only communication that survived besides the runner. Cell phone service was clogged and then stopped working. Because many of the responding units did not have the same radios or use the same radio frequencies, radio communication was chaotic. Runners were used to transmit information between the 24 incident command posts. Twenty-four command posts, rather than one were set up because of communication difficulties. In addition to improving phone and radio emergency communications through dedicated bandwidth, we ought to exploit the Internet and area networks for data, picture and voice communications. One can imagine that a major airport incident or airline destruction with terrorist origins would present the same sorts of communications issues that I just described. But such technology can also be used to prevent such incidents through realtime collection and correlation of passenger information that can detect and identify potential terrorists.

Some of the capabilities now available which would address aviation safety are local wireless area networks (LAN), and hand-held or laptop computers connected to these wireless LANS for local communications. These technologies are affordable because of economies of scale; future offices and homes will all be using wireless data communications to avoid the current maze of wires and to improve mobility. Such configurations can also be easily connected to the Internet or other wide area

network (WAN) for communications from an airplane or airport to sources of data, expertise and help. Such configurations are not susceptible to telephone jams or radios which cannot transmit or receive on the same frequencies; they are also less susceptible to radio interference. LANs will work as long as local power is available and could be powered by emergency generators. Internet II will provide dedicated bandwidth for emergency data transmission. Data formats and protocols are standard around the world, so any organization responding to an emergency could be easily interoperable.

Last November, Georgia Tech CERTIP demonstrated the use of local wireless networks, laptops and handheld computers, and Internet connectivity to improve communications at a simulated CBRNE incident. All of the first responders at the incident site could exchange data through the LAN and could communicate with anyone in the world using an Internet hook-up. Most of the data we chose to transmit were medical data but any type of data could be exchanged. For example, airports and airplanes can use such information technology configurations for realtime collection and analysis of passenger data to detect potential terrorists and to coordinate emergency response with local, state and Federal response organizations. Passenger screeners can easily enter information on the results of passenger searches through handheld computers; airport personnel can contribute information about suspicious activities.

Information technologies can also assist in tracking down those exposed to biological agents. Georgia Tech CERTIP, in collaboration with the CDC and Dekalb County Public Health Service is planning to demonstrate the use of information technology to accelerate the epidemiological investigation of infections diseases, starting with West Nile virus. But such techniques could also be used to help stop the spread of biological agents such as smallpox.

(4) *Training* of personnel is a key issue in aviation safety. Recent law will require the Department of Transportation to hire large numbers of passenger screeners and air marshals. Fortunately, there are commercial and emerging instructional technologies which can help train these new employees. Georgia Tech has gained experience with such technologies to aid learning on our campuses and to help other organizations. For example, web-based training is now a reality for many employees in many places including large-scale DOD systems.

Given the accessibility of the World Wide Web to corporate and government entities, this avenue for delivering training holds promise not just for conveying content in an interactive manner, but also for maintaining electronic records of trainee performance.

With access to streaming video and other bandwidth-intensive applications, it is now possible to generate on-line simulations that can test the responses of individuals and groups to multiple scenarios at multiple points in each scenario. Such structured exercises can be used to teach trainees how to respond to routine and exceptional events, and how to distinguish easily between them. The fact is that the web is worldwide means that the physical location of the trainee is of no consequence with respect to accessing the training materials. Also, because technology-mediated learning allows for individualized tutoring applications, any trainee who needs extra practice with or exposure to the training materials can be easily accommodated. The testing module itself can be configured to perform diagnostic analyses that will inform learners of their weaknesses and advise them on steps they can take to improve their performance that are consistent with individual learning styles. These applications can be easily customized to the needs of individual learners. Finally, a web-based application can be archived so that competency levels of trainees can be easily surmised from the archival records.

Again, thank you Senator Cleland for your support of Georgia Tech and homeland defense.

Senator CLELAND. Well, thank you very much, Doctor, and Georgia Tech, I am sure, will be called upon in the coming years to be extremely helpful here because this is one area where technology can be of tremendous help.

This trusted passenger concept where you have people willing to go through a background check or have their fingerprint ID'd or retina scanned or whatever it is, and they carry that technology with them on their person. Do you see potential for that technology to be helpful in the customer service area of expediting this security check?

Dr. BEVAN. Yes, I think smart cards with information on them to help, in combination with biometrics, can give you very good confirmation that that is the person he says he is or she says she is. The thing we have to do is work—the concern from a sociologic point of view, we have a very strong streak in America of not wanting to have national ID cards, we do not like that very much and we do not want to appear to also have a two-tiered system of security—one for some people and one for another.

Senator CLELAND. Thank you very much.

And now we get to our pilots. We do not get very far without the pilot cranking that engine up and saying we are ready to go. Mr. Kevin Macginnis is with the Air Line Pilots Association and the Delta Master Executive Council and we are glad to have your statement, please.

STATEMENT OF KEVIN D. MACGINNIS, MEMBER, AVIATION SECURITY COMMITTEE, DELTA PILOTS MASTER EXECUTIVE COUNCIL, AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Mr. MACGINNIS. Good morning, Mr. Chairman. My name is Kevin Macginnis and I live in Peachtree City, Georgia, I fly for Delta Air Lines as a co-pilot on the MD–88. I am based in Atlanta and fly extensively out of Atlanta Hartsfield International Airport. I am a member of the Aviation Security Committee of the Delta Pilots Master Executive Council of the Air Line Pilots Association.

Captain Stock Coleman, who is my boss, regrets not being able to be here today. He is currently over in Tel Aviv attending a security conference held by El Al Air Lines.

You have my written statement for the record and I would like to briefly highlight some of the key elements.

When President Bush signed the Aviation and Transportation Security Act into law, the foundation was laid for the creation of an aviation security system that provides real security with the lowest possible degree of intrusive procedures. We applaud the U.S. Senate for your expeditious and unanimous support of this important legislation.

As we develop a structure that will stand on this foundation, we pledge the continued support of over 60,000 professional aviators who are members of the Air Line Pilots Association.

When I fly to any of the hundreds of commercial airports across the country, I communicate with air traffic controllers who use common phraseology in their transmission and follow procedures that are national in scope. A clearance to make an instrument approach, for example, means the same thing in Portland, Maine as it does in Portland, Oregon.

Aviation security, however, is a different matter. Prior to the 11th of September, the level of security varied considerably from airport to airport on the basis of what has been called local perceived threat. As we continue the regulations and construct them, that will implement the Aviation and Transportation Security Act, let us recognize that a terrorist who enters our system in Albany, Georgia presents no less of a threat to the national security than a terrorist who enters the system in Albany, New York. We must begin from the premise that the concept of local perceived threat is a dead letter.

We urge the creation of one level of security that applies at every airport and air carrier nationwide. There should be no difference in the security standards that are applied at small airports and those that apply at large ones. There should be no difference between the security standards that apply to small airlines and those applied to large ones. We should also understand that a Boeing 777 from Delta Air Lines and a Federal Express DC–10 would make equally lethal terrorist missiles. Therefore, there should be no difference between the security standards that apply to passenger operations and those that apply to cargo operations.

There is an Irish toast that goes, "Here is to those who love us; and for those who do not, may the good Lord turn their hearts. But if he does not turn their hearts, may he turn their ankles, so that we will know them by their limping."

We should allow our security personnel to better focus their efforts in screening of people who are unknown by reducing the level of scrutiny that is applied to people we already know and trust. When I report to work at any airport in the country, I am likely to spend a fair amount of time in a long line only to have my flight kit emptied and my overnight bag searched, just to make sure that I am not carrying anything that I could use to commandeer the airplane upon which I am legally assigned second in command.

Of course, the security personnel who search my bags certainly have no independent way to verify that I am who I say I am. If we did not know better, we would assume that there was not any simple way to separate the wheat from the chaff, pilots, flight attendants, ramp workers and law enforcement officers from the general public. But the truth is that the technology exists today for a combined computer chip and biometric verification system that could be implemented expeditiously and economically.

A system could be implemented that would allow me access to a secure area based on a swiped card and a fingerprint scan that would generate my picture and employment status on a security monitor that would be monitored by a security officer and that would happen both at the gate and when we come through security.

Many of my colleagues and I became airline pilots after we served long military tours where we held top secret clearances and were entrusted with weapons of mass destruction. We passed extensive background checks then and again when we were hired by Delta.

We also need a way to know that the baggage in the cargo hold contains no device that is intended to cause destruction of the aircraft, its passengers and its crew. Until such time as we are able to implement this universal baggage screening, we urge the creation of an inexpensive photo manifest in order to quickly remove any bag in the event its owner does not board. Aviation safety is based in part on multiple redundancies, so that if one system fails, there is a backup to prevent a catastrophe. In the cockpit, we have two altimeters, two air speed indicators and two yokes. The aircraft has two hydraulic systems, two engines, two air/ground safety sensors.

The ultimate redundancy in aviation security must include both an impregnable cockpit and the ability of the flight crew to respond

to a threat in the gravest extreme. If we are prepared to scramble U.S. fighter jets to intercept a commandeered commercial passenger aircraft, ought we not provide the crew with equipment and training that is sufficient to eliminate a threat short of destruction of the aircraft?

Thank you very much for the opportunity to share the views of the Air Line Pilots Association this morning and I will be happy to answer any questions.

[The prepared statement of Mr. Macginnis follows:]

PREPARED STATEMENT OF KEVIN D. MACGINNIS, MEMBER, AVIATION SECURITY COMMITTEE, DELTA PILOTS MASTER EXECUTIVE COUNCIL, AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

I am Kevin Macginnis, a member of the Aviation Security Committee of the Delta Pilots Master Executive Council of the Air Line Pilots Association, International. I also serve as Chairman of the Aviation Security Committee of ALPA Council 44. Council 44 represents more than 4,000 Atlanta-based Delta pilots. ALPA represents 67,000 airline pilots who fly for 47 U.S. and Canadian airlines. We are sincerely appreciative of the opportunity to appear before the Committee to present our views on the important subject of aviation security.

ALPA has been at the forefront of the effort to create a more secure airline travel system. We are pleased, therefore, that the President, on November 19, 2001, signed into law P.L. 107–71, the Aviation and Transportation Security Act, which contains many of the provisions we had urged be adopted.

This hearing is most timely, in that it concerns the actual implementation of that law's numerous provisions and other initiatives. Congress' oversight role will be critically important to prevent a repeat of some of the FAA's regulatory missteps in years past. One example of such a misstep was the agency's failure to produce major security regulations in a timely manner—revised CFR 14 Parts 107 and 108 were published this summer, 10 years after revisions began! We are hopeful that the new DOT Under Secretary's office will produce NPRMs and final rules in a more expeditious fashion.

For many years, ALPA has promoted One Level of Safety for all air carriers carrying passengers or cargo in the United States. We, therefore, strongly support One Level of Security during the implementation of Federal security-related regulations. Instituting a single security level, by definition, means the abolition of today's sundry security levels and practices for airlines and airports based on perceived threat. A terrorist-guided missile, in the form of a fully loaded airliner, can take off from any commercial airport in the country and wreak havoc on unsuspecting innocents virtually anywhere below. A suicidal bomber can affect a terrorist attack as decisively on an airplane departing from Des Moines as one leaving from Dulles. There is no difference between a fully loaded B–747 cargo airplane and a fully loaded B–747 passenger airplane in terms of their use as terrorist missiles. Each of our recommendations is made in this context.

Following are some specific initiatives we believe need to be addressed in the implementation of the new law.

EMPLOYEE AND PASSENGER IDENTIFICATION

ALPA has been promoting the need for positive, electronic verification of identity and electronic airport access control systems since 1987—shortly after the downing of PSA flight 1771 by an armed, disgruntled, former airline employee. This mass murder, which bore similarities to the hijackings of September 11th, was attributable in large measure to identity-verification inadequacies that have yet to be addressed 14 years later.

At ALPA's urging, the FAA required approximately 200 of the largest commercial airports to install computerized access control systems in the late 1980's and early 1990's. However, in spite of the entire aviation industry's arguments to the contrary, the agency failed to (1) create a detailed set of performance standards for use by the airport community and (2) provide for the access control and identification needs of the transient airline employee population. This mismanagement was, and still is, expensive for the airports and airlines—the initial estimate of about $170 million for access controls actually rose to more than $600 million, and the figures continue to climb. There are also numerous costs that are difficult or impossible to compute stemming from the inefficiencies related to transient airline employee's lack of access at airports.

In the mid-1990's the FAA, with ALPA's urging and congressional funding, performed a test of what came to be known as the Universal Access System (UAS). Two million taxpayer dollars were spent on those tests involving two major airlines and four large airports. For all practical purposes, those funds were wasted. Although the FAA completed successful tests of the UAS and standards were finalized for the system in 1998, there has been no implementation by any airline of the system, per stated congressional intent. This failure came as a result of an FAA policy to leave UAS implementation to the sole discretion of the carriers.

Although magnetic stripe technology was used as the basis for UAS tests, there are now several advanced, mature technologies that could be used to positively identify authorized personnel. The FAA is expected to complete a study of its recent tests of a Memory Chip Card (MCC) system for identifying armed law enforcement officers in the near future. This technology is much more secure than magnetic stripe and has the additional capability of storing an extensive amount of data that can be used for both security and other types of uses.

The FAA has stated that these same readers could also be used by airlines for issuance of MCC cards to their employees. ALPA is recommending that the airlines use the MCC, or an equally secure technology or technology combination (e.g., smart card with biometric reader), as the means for performing several important functions, including the following:

1. *Positive access control for all employees who work at the airport, not just non-transients.* Airline pilots and other transient employees currently rely on a very non-secure method of moving around airports, which creates the potential for security breaches. Namely, they request airport-based, company employees to open doors for them as a courtesy based on their possession of an airline ID card. As we know, ID cards and uniforms could be fraudulently used to gain access, which underscores the need for electronic verification.

2. *Positive verification of identity at the screening checkpoint to enable transient employees to be processed more quickly.* Passengers are enduring long lines at the security screening checkpoint. These lines are made longer by the screening of pilots, flight attendants and other individuals in positions of trust, who are often screened several times a day. The lack of equipment for positively identifying these individuals wastes limited screening resources and further inconveniences the traveling public.

3. *Identity verification of jumpseat riders.* Use of the jumpseat by commuting pilots is an absolute necessity in today's airline environment. Unfortunately, that privilege has been severely curtailed since shortly after the terrorist attacks because there is no way to positively verify the jumpseat requester's identity and employment status.

4. *A platform for digital pilot licenses and medical information.* Consistent with language in the Act, we recommend that the same card, or type of card, be used by the FAA for containing a pilot's license and medical information. ALPA is working with FAA Flight Standards on this concept. Smart cards have more than sufficient memory for this purpose and others that the airlines may develop.

One important aspect of access control systems and UAS is the need for specifying a *single* set of performance standards to be used by all equipment suppliers and system integrators. Different types of technologies, used by different airports and airlines, can be incorporated into the aviation security system *if* interoperability is a requirement for all of them. RTCA, an aviation standards organization, may be useful in helping to create such standards.

In concert with the new security law's provisions regarding passenger identification, several organizations are promoting "smart" cards for passengers to be read at the screening checkpoint. Conceptually, such individuals would be processed more quickly than those without a card at a special lane created for this purpose. ALPA supports this recommendation provided that the passengers voluntarily submit to a thorough background check and, if possible, a criminal history records check, in order to receive this card. The background check should be updated at least annually in order to retain it.

Evidencing the importance of this issue, nine of the 33 DOT Rapid Response Team (RRT) recommendations relate to the subject of employee and passenger identification and access control, namely: Aircraft Security Report recommendations 7 and 8; and, Airport Security Report recommendations 2, 4, 7, 8, 9, 13, 16. A copy of these recommendations is included with my statement.

We recommend that the government amend CFR 14 FAR Parts 107 and 108 to accomplish the following:

1. Identify a single performance standard that will be used by access control equipment providers and integrators, the airlines and airports to create a universal access system.

2. Require airlines and airports to create such a universal access system that incorporates, at a minimum, the following features: (1) can be used by any transient airline employee at any U.S. airport where they operate (2) requires the carriage of only one piece of media (e.g., smart card) (3) positively identifies pilots for jumpseat-riding purposes (4) allows the bearer to open all access-controlled doors to which they have authorized entry (5) allows the electronic storage of pilot license and medical certificates, and (6) is used as the principal means of processing transient employees through the security screening checkpoint.

3. Establish a provision within FAR Part 108 that will allow the creation of a "trusted passenger" identification and security screening checkpoint methodology aimed at increasing security and checkpoint throughput.

HIRING CRITERIA AND PERFORMANCE STANDARDS

The foundation of a good security system for any entity, public or private, is a sound set of hiring criteria. Non-trustworthy employees cost time, money, and in the most extreme cases, can be life-threatening. The aviation industry has failed in several respects to ensure that only the most trust-worthy individuals are hired into critical, security-sensitive positions.

Background checks, consisting mostly of employment verification, have been used by the aviation industry for a number of years. These checks have more recently been supplemented by criminal history records investigations when a lapse in employment has occurred or there is some other questionable matter associated with an applicant's past.

It is our recommendation that criminal history records checks be performed on all new employee applicants to help ensure that only the most ethical and trustworthy employees be allowed within airport secure areas. Unfortunately, the issue of background and criminal history checks is greatly complicated by non-U.S. citizens and those who have been U.S. citizens for only a short time.

Accordingly, we recommend that the government amend CFR 14 FAR 107 and 108 to require mandatory pre-hire criminal history records check for all applicants who are U.S. citizens. An Interpol criminal history records check should be performed on all applicants who are either not U.S. citizens, or have not been U.S. citizens for at least 10 years. We endorse the Act's specific provisions for screener hiring standards.

Performance standards for baggage screening can best be tested and monitored through use of the Threat Image Project System, or TIPS. TIPS intermingles images of bags containing threat objects at random with the x-ray or EDS images of real bags. Screeners are required to identify the threat objects in a TIPS image, just as they do in a real bag, and their results are quantified and logged by computer. Performance of screeners has been shown to substantially improve with TIPS technology and it should be made a mandatory component of all baggage screening equipment.

EMPLOYEE TRAINING

Pilots at many U.S. airlines view the security training that they receive from their companies as boring, irrelevant, and unrealistic—much of it is repetitive from year to year and may largely consist of watching video tapes. Accordingly, ALPA wholeheartedly endorses the new provision contained in the Act that calls for the government and industry to develop "detailed guidance for a scheduled passenger air carrier flight and cabin crew training program to prepare crew members for potential threat conditions." We recommend that new regulations also provide for security training of all-cargo pilots, who have special requirements in this regard.

An Air Transport Association (ATA) working group has recently developed, with our input, a very brief response to the RRT on Aircraft Security recommendation number 12. That response, however, does not fulfill the requirements of the Act for a number of reasons, not the least of which is that it does not identify an adequate response to acts of air piracy. ALPA has scheduled a meeting to occur in a few days with FBI, FAA, Secret Service, and other government and industry organizations to develop a new "Common Strategy" that can be used for training airline personnel on air piracy strategies. A revised Common Strategy is needed to develop many of the training elements that Congress has identified.

We recommend that FAR Part 108 be amended to specifically require that airlines incorporate all of the program elements identified in the Act, plus any additional elements that may be identified during the rulemaking process.

BAGGAGE AND CARGO SCREENING

ALPA endorses the new security bill's provisions to require security screening of all checked bags loaded onto passenger-carrying aircraft and the screening of cargo and mail on cargo aircraft. The potential for carrying a bomb-laden bag onto an aircraft is very real and needs to be addressed expeditiously.

The new security law provides the Under Secretary with a 1-year study period for reporting on the screening requirements applicable to aircraft with 60 or fewer seats used in scheduled passenger service. We recommend that all baggage of all airline passengers be screened, regardless of the size of aircraft on which they fly. Also, as we understand the Act, there will be some passengers who travel on small aircraft from certain points of origin without benefit of security screening who will be charged as much as $5.00 for security services on a one-way trip. This situation may be as the result of an oversight, but it is one that deserves the attention of Congress.

We recommend that Congress quickly take this issue up and provide legislation that will ensure that everyone who travels on U.S. commercial aircraft, and pays a security fee, is provided the same level of security.

ALPA has for several years promoted the concept of creating an electronic passenger and baggage manifest. Similar to the problem of employee identity verification, the airlines are not currently capable of positively determining who has boarded their aircraft. This is demonstrated when aircraft leave the gate with an inaccurate manifest; we know of one airline that routinely allows flights to leave the gate with up to a two-person error. As another example, after one accident last year, an airline CEO made a public request for assistance in identifying the passengers on his own aircraft! The security ramifications are also substantial—unless we know that the person boarding the aircraft is the same one who bought the ticket, we cannot positively determine that the individual has been through the security checkpoint.

Currently available technology can be applied to this problem in order to create an inexpensive photo manifest of boarding passengers and their checked bags. The photo manifest will enable airlines to, among other things, (1) positively identify each person and bag on the aircraft (2) reduce the potential of boarding someone who has not been through screening (3) create a strong deterrence against fraudulent ticketing (4) quickly identify a bag(s) that must be removed in the event that its owner does not board the flight (5) create an accurate passenger manifest that can be used in the event of an accident or other tragedy and, (6) if tied to appropriate data bases, identify those of possible criminal intent.

ADDITIONAL MEASURES IN THE AVIATION AND TRANSPORTATION SECURITY ACT

I would like to turn your attention now to the need for additional regulations for implementing certain provisions of the Act. ALPA has been heavily involved in the development of, and responses to, the security recommendations of the DOT Rapid Response Teams (RRTs), and I would like to address the status of some of those recommendations as part of this discussion.

Aircraft Cockpit Hardening

We are encouraged by the rapid move toward full, voluntary fleet compliance with Special FAR 92–2, which FAA recently issued. Today, nearly every U.S. passenger airliner has been modified to provide better, although temporary, security of the flight deck. Modification of the cargo fleet, although allowed by SFAR 92–2, was not supported by FAA funding, as was the case with the passenger aircraft fleet. As a result, modifications to cargo airlines' cockpit doors lag those of the passenger aircraft. It is important that cargo aircraft cockpit doors be strengthened for several reasons, including (1) cargo aircraft are subject to air piracy, just like passenger aircraft (2) security protecting cargo aircraft is nearly always less stringent than for passenger aircraft (3) cargo flight crews are often required by their companies to board additional, non-screened employees or couriers, about whom the pilots may know little or nothing, in seats outside the cockpit door.

The process to institute permanent cockpit door design changes referred to in the Act and in DOT aircraft security RRT's recommendations two, three, and four has already begun. A recent regulatory proposal by the ATA would provide for improved security of passenger airliner flight decks. Once again, however, the proposal does not include cargo carrier aircraft. The RRT recognized the need for improvements to both types of transport aircraft doors when they specified, "retrofit of the entire US fleet" in their recommendations.

Furthermore, the ATA proposal stops short of requiring complete protection against gunshots, grenades, and other explosive devices. The design standards pro-

posed for *new* aircraft provide such protection calling for "hardening" of cockpit floors, ceilings, and bulkheads, but retrofit of that protection is not addressed in the ATA proposal. This is a serious issue—many aircraft in the fleet today, thus exempt from regulations covering new designs, will likely be flying for decades to come. The number of aircraft of new design will be miniscule by comparison.

We note that the Act legislates "such other action, including . . . flight deck redesign, as may be necessary to ensure the safety and security of the aircraft." This language is consistent with aircraft security RRT recommendations two, three and four—to provide one level of security for every U.S. airliner, regardless of whether it is being flown today or still on the drawing board, for both passenger and cargo aircraft alike.

We recommend that new Federal regulations address the need for enhanced flight deck security on today's fleet of aircraft, not just those aircraft of tomorrow.

The Act also calls for an investigation by the Administrator for determining a means of securing the flight deck of smaller passenger aircraft that do not have a door and a lock. These aircraft are particularly vulnerable, because many of them do not even have a flight attendant who can help prevent, or alert the pilots to, a security problem. New regulations should be developed that will ensure one level of security in this area.

Cabin Monitoring and Emergency Warnings

The Act provides for the use of "video monitors and other devices to alert pilots in the flight deck to activity in the cabin." The industry has held discussions about two related RRT recommendations, and there are numerous vendors with products that will address them, from the simple to complex. We recommend implementing regulations that are broad enough to allow airlines some latitude in selecting those products and systems that will work best for a given type of aircraft in the company's fleet. Pilot input should be solicited in the development of any such security enhancements, as they will be the ultimate end-user of them.

Even though video monitors may have a role in our aircraft cabins, we are duly concerned about the ultimate, improper use of any video recording. The recent television airing of recordings made during the struggle aboard United flight 93 on September 11th demonstrates that some within the media will not respect human dignity or decorum on a voluntary basis. We are adamantly opposed to any new type of audio or video recording device on aircraft unless all appropriate legal protections are in place in advance to prevent such recordings from misuse by the media, airlines, or government agencies.

Defensive Capabilities for Pilots

ALPA is most pleased that Congress agreed with the need for providing pilots a means of voluntarily arming themselves with lethal force. The Act's language in this area leaves considerable flexibility in how it may be implemented. We are currently studying this subject and intend to create a set of recommendations on what types of weapons should be carried, how the weapons should be transported, training curriculum and other related subjects. We plan to promote our views to the office of the new Under Secretary and appropriate FAA offices for their consideration in developing regulations.

We would note two specific omissions in the Act regarding carriage of lethal weapons by pilots. First, there is no provision in the Act for an exemption from liability in the event that a pilot uses a lethal weapon in self-defense. Second, the Act does not create a Federal exemption from State laws for interstate carriage of weapons. We call on Congress to write new legislation aimed at addressing both of these requirements.

Regarding non-lethal defensive capabilities, discussions are ongoing with others in government and industry on the best means of providing such to both pilots and flight attendants. The discussions are not yet mature enough for regulations, consistent with the Act's provision for a study by the National Institute of Justice on this matter.

Passenger Volunteers to Provide Emergency Services

We endorse the Act's provisions for passengers to volunteer their services in the event of an emergency. This security enhancement is one that ALPA has promoted for several years. The Act's language, however, is very narrow in that it limits the volunteers to law enforcement officers, firefighters and emergency medical technicians. Notably absent are others, such as doctors, bomb technicians, and able-bodied individuals, who could provide useful services in the event of various types of emergencies.

We recommend that Congress broaden the scope of this legislative language to include additional categories of volunteers. We also recommend that these individuals,

if they pass requisite background and criminal records checks, be identified as volunteers via future "trusted passenger" cards. The information about their special abilities could be stored on a smart card that would be read by airline personnel and, eventually, be transmitted to the captain for his use as necessary.

Aviation Security Programs for Air Charters

ALPA endorses the Act's provision for air charter security programs. Under current regulations, large commercial aircraft can be operated with little or no security provisions because of their charter status. Clearly, new regulations are needed to ensure that the same level of security for scheduled operations is provided for non-scheduled operations.

OTHER ISSUES

Last, I would like to bring to your attention a couple of other issues that are not included in the Act, but we believe they are worthy of your consideration.

INS Deportees

ALPA has a long-standing concern about the use of airline aircraft to transport Immigration and Naturalization Service deportees out of this country. While the INS has, in our opinion, taken some steps to be more responsible with these "voluntary" deportations on our aircraft, the potential for problems still remains. In our view, anyone who is required to leave the country involuntarily is a security risk; they are traveling against their wishes to a destination where they may face prison or other hardships. A natural incentive is created for these individuals to try to escape or alter their travel destination. Many of the deportees carried aboard our aircraft have some type of criminal records and it is not uncommon for them to also have medical problems that are not conducive to passenger health. Buttressing these concerns are actual instances of sexual assaults, lewd behavior and other problems.

Under INS regulations, no escorts are provided for deportees unless they are deported in groups of 10 or more. We recommend that the INS find other means of deporting these individuals without subjecting the traveling public to potential for harm. Alternatively, deportees should not travel on commercial aircraft unless they are escorted by two or more individuals who are assigned to control them from the moment of boarding until disembarking.

We recommend that Congress address this matter immediately with legislation aimed at eliminating the INS' deportation deficiencies.

Security Information

Aircraft Security RRT recommendation number 13 recommends that each airline develop a delivery system or procedure to provide government security advisories to crewmembers in a timely manner. Currently, many pilots receive no timely security information at all. Some airlines, which can legally provide information from security directives to pilots because of their "need to know," instead withhold that information.

A regulation needs to be added to CFR 14 FAR Part 108 to require that airlines provide captains with all appropriate information about new security provisions, potential areas of threat, and other related subjects.

Thank you again for the opportunity to testify today. I would be pleased to address any questions that you may have.

Senator CLELAND. Thank you very much, Mr. Macginnis.

Several cockpit issues—first of all, I think the airlines have dealt well with the cockpit security issue. You mentioned that your boss was going to El Al—to Tel Aviv. El Al is a small airline, so I am not sure you could exactly replicate this, but in terms of cockpit security, they have actually two doors to the cockpit. It is almost like a submarine airlock where you enter an outer door, you come in, that outer door is then electronically and/or manually locked and then you enter the cabin and in effect the pilots and the co-pilots have access to the bathroom and so forth through the inner secure sanctum area. They never go outside into the cabin. So once they are in, they are in and nothing will get them out. And their job is to land the aircraft, that is the El Al standard. The air marshals which are on every El Al flight, their job is to control the cabin.

I know that is maybe a little bit much, but in your opinion, in regard to the security of the cockpit door, are you pretty much comfortable with where we are now or do we need to do more?

Mr. MACGINNIS. Yes, sir, we are very comfortable where we are now. New standards are being developed for an improved cockpit door that would be more beneficial and give us more safety features than we currently have in place now. Obviously we have more sky marshals that are flying on our flights today. That is also an added benefit there. But there is still more that needs to be done, including the voluntary arming of flight crew members.

Senator CLELAND. Yes, I want to get to that in just a minute.

Redundancy—do we need two transponders? You mentioned the duality of things in the cockpit. Part of the challenge on September 11 was that the hijackers turned the transponder off. The FAA, in effect, had to play a passive role and could not really track these aircraft and even if they were able to call upon an F–15, they were not able to track them. As you fly in American airspace, do we need some transponder that is on all the time so that the FAA is able to find an aircraft wherever it is in the sky?

Mr. MACGINNIS. We currently have transponders that once we basically take off to landing, that track us throughout the skies, our every movement. However, the incident on September 11, they were able to turn that off. There is technology now that prevents that system from being turned off in the event of an emergency.

Senator CLELAND. That is good to know.

Now, stun guns in the cockpit. How do the pilots feel about weapons, stun guns, that kind of thing in the cockpit?

Mr. MACGINNIS. My prior experience as an FBI officer working on operation safety task forces, you come up with operational procedures for each weapon that you use. With the stun guns, the current operation procedure is that you have two officers that have lethal force standing by in case the stun gun does not work.

The Air Line Pilots Association is similar to that of the FAA requirement having a fire extinguisher in the aircraft. We have a fire extinguisher up in the cockpit; in case there is a fire, one person flies the airplane and the other one puts out the fire. If an intruder were to come through that cockpit door, we would have one person to fly and we would like to have the fire power to put out that fire if that person ever came through.

Senator CLELAND. Thank you. Well, thank you very much for your testimony and thank you very much for your work.

Mr. Planton, thank you very much for your patience. Mr. Jeff Planton is a Senior Vice President, EDS (Electronic Data Systems).

Mr. PLANTON. Yes.

Senator CLELAND. Now there is an acronym EDS that has to do with demolitions or identifying——

Mr. PLANTON. Explosion detection system, yeah.

Senator CLELAND. So you are not the explosion identification people.

Mr. PLANTON. No, we are not.

Senator CLELAND. You are the Electronic Data System.

Mr. PLANTON. And we usually make that distinction in these hearings.

Senator CLELAND. Thank you and welcome.

STATEMENT OF JEFF PLANTON, SENIOR VICE PRESIDENT, ELECTRONIC DATA SYSTEMS (EDS') U.S. GOVERNMENT GROUP

Mr. PLANTON. Thank you. I guess I can say good afternoon officially, Senator Cleland.

Senator CLELAND. Yes, sir.

Mr. PLANTON. My name is Jeff Planton and I am Senior Vice President of EDS's U.S. Government Group and I am based out of Herndon, Virginia.

We appreciate the opportunity to present our views to this Subcommittee and on the subject of great importance to our country, to our company and to our customers.

Following the worst threat and terrorist asttacks in U.S. history, the Federal Government, airports and the airline industries are grappling with short and long-term solutions to improve and enhance passenger safety.

Since September 11, EDS has been involved at many levels with our government and private sector clients, which include the Federal Aviation Administration, Immigration & Naturalization Service, domestic and international airports and some of the largest airlines in the world. Immediately after September 11, EDS assembled a team representing every element of the aviation industry and critical technologies including biometrics, smart cards, information security, complex data management and airline specific systems.

Our team has identified an approach to aviation security that encompasses the passenger experience, the airport environment and the underlying infrastructure. Today's testimony covers the passenger experience and portions of that recommended infrastructure.

First, we should address the current situation. Industry capacity has been cut by 20 percent—80,000 employees have been laid off, hundreds of aircraft have been parked and orders for new aircraft delayed or canceled. In order for Americans to get back into the skies, they need to feel better about what has been done to improve airline safety.

The good news is, with sufficient assurances of safety and service, pent up demand could quickly outpace recent capacity cuts and we could return to new levels of what we saw before September 11. To achieve this, we must improve existing physical security with a balanced approach of innovative processes and proven technologies.

To date, priority has been given to physical security measures such as National Guard troops in airport terminals and more rigorous searches at checkpoints and gates. These visible measures appear to be improving passenger confidence; however, these advances in passenger confidence have been offset by declines in customer service and convenience. The traveling public has been very patient with increasingly intrusive and time-consuming searches, but they are starting to complain about pat-downs and even requirements to unbutton clothing at gate areas. Clearly this is not a system that is a viable long-term solution.

To stimulate air traffic near the pre-tragedy volumes, we must stimulate and address confidence and convenience. The Aviation and Transportation Security bill references solutions that help us accomplish these objectives. Among other things, the bill calls for

trusted passenger programs, improved baggage management processes and enhanced passenger pre-screening systems. We fully support these initiatives because they address fundamental security questions—who they are and who they say they are; are they a threat to security; and are they carrying anything illegal. They also leverage proven technologies that can be rolled out quickly.

In a new era of suicide terrorists, positive identification of passengers is as important as the detection of bombs and weapons. Currently, traditional identification documents like drivers license or passports are the only means of validating identity of passengers. Yet these documents are easily stolen or forged. Recognizing this, we now have to treat all passengers as high risk. This means more random searches, more inconvenience for law-abiding citizens and perhaps worst of all, more wasted time for security personnel who should be focused on truly high-risk passengers.

EDS joins other industry partners and other aviation associations in recommending opt-in process to increase the number of known or trusted 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 traveler because the known persons are removed from their queues. And third, it increases security for all because security resources can be focused on a smaller universe of unknowns.

The cornerstone of the trusted traveler program is a voluntary biometric identity system. These systems could be used to speed check-in and process for frequent travelers, who represents as much as 50 percent of the flying public. Having once registered with the system, where full proof of identity was provided and a background investigation successfully completed, a traveler would be issued a smart card. With this card, the passenger can authenticate his or her identity in seconds at a biometric checkpoint using biometric technologies such as fingerprint scanning, hand geometry or facial recognition.

EDS has such a system in place today at Ben Gurion International Airport in Israel which is considered the safest airport in the world. It allows registered Israeli citizens to authenticate their identities with a magnetic card in a biometric technology, saving up to 2 hours off the wait at passenger 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.

While the current FAA-mandated computer-aided passenger prescreening, CAPS, is a great start, the regulators, airlines, unions and associations agree that improvements are warranted. EDS recommends a centralized passenger evaluation system that will objectively evaluate the level of risk that each individual poses to the transportation system. With a centralized system, risk criteria could be changed near real time and could instantaneously alert all airlines of the potential threat. Further, this system would be the foundation for comparison of passengers to law enforcement watch lists.

This kind of system is not new. In fact, EDS currently is operating a similar prescreening system for a number of U.S. airlines, processing approximately 70 million passengers annually. Given that number of airlines already utilizing the system, EDS feels that a version of CAPS is the logical foundation for a national passenger evaluation capability and could be deployed in about 6 to 9 months, depending on final requirements and funding arrangements.

EDS also recommends a flight risk management solution that aggregates individual risks into an overall flight or airport risk situation. This solution would provide airports with information on when to escalate security measures.

As the Aviation and Transportation Security Act requires, all checked bags should be screened, using expolsive detection equipment, EDS.

[Laughter.]

Mr. PLANTON. However, after 100 percent screening is achieved, systems must be implemented to ensure the integrity of those bags. Once a bag has been cleared of explosive materials, it needs to be secured, either by sealing the bag itself or sealing it within a luggage container. After being sealed, the bags or containers could be tracked and tracked throughout the airport using bar codes or radio frequency identification devices, RFID tags like the tags you put in the window of a car. Using this technology, airports and airline personnel would know whether a specific bag that arrived at the plane should have arrived. If it did not, they could determine where the bag was removed from the process and why. This form of electronic tracking also facilitates a positive bag match to those actually boarding the aircraft and allows personnel to quickly locate that bag and remove it from unattended checked baggage. This same system could be used to secure and monitor cargo and mail.

A number of baggage identification, sortation or reconciliation systems are in place today, both here in the United States and around the world. Many rely on bar code technology, although RFID bag systems are being piloted by several airlines today. Further, RFID is proven technology frequently used in other industries, especially assisted in tracking and monitoring vehicles, inventories and managing supply chains.

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 the key component of a security screening process. However, technology will be critical to the solution that enhances security while preserving the convenience, privacy and fiscal responsibility. It is imperative that a solution to aviation security be approached from an enterprise perspective. Such an information system will have to process real time data, must be accessible to airports, airlines, governments around the world, robust systems permitting central data management with greatly distributed data collection required. This system will require a solid infrastructure with no possibility of down time, and without question, access to it and 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 hundreds of thousands of biometrically enabled smart

cards for the U.S. Department of Defense. EDS prescreens millions of passengers using its client server CAPS system every year. Ben Gurion International Airport utilizes a biometric system to expedite immigration of 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 millions and millions of products in the United States and abroad. Beyond the individual solutions, the scale and scope of the system would not be unprecedented either.

While integration of such disparate data bases and complex technologies on a global scale might be new for airports and the airline industry, global service providers like EDS already have extensive experience creating and running comparable systems in other industries.

The challenge is to restore the confidence and the convenience at the same time. Logic dictates that restoring one without the other will not solve any of the problems we face and the solutions I have described today would complement physical security enhancements and compensate for the negative impact on services. By implementing these solutions, we will restore confidence to the flying public and get Americans back in the skies.

Thank you very much and I will answer any questions you have.

[The prepared statement of Mr. Planton follows:]

PREPARED STATEMENT OF JEFF PLANTON, SENIOR VICE PRESIDENT, ELECTRONIC DATA SYSTEMS (EDS') U.S. GOVERNMENT GROUP

"NEXT STEPS IN AVIATION SECURITY: RESTORING CONFIDENCE AND CONVENIENCE"

Good morning. My name is Jeff Planton and I am a Senior Vice President of EDS' U.S. Government Group based in Herndon, Virginia EDS appreciates the opportunity to present our views to this subcommittee on a subject of great importance to our country, our company and our customers.

Following the worst terrorist attacks in U.S. history, the Federal Government, airports and the airline industry are grappling with short- and long-term solutions to improve and enhance passenger safety. Since September 11th, EDS has been involved at many levels with our govornment and private sector clients, which 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.

Immediately after September 11th, EDS assembled a team representing every element of the aviation industry and critical technologies, including biometrics, smart cards, information security, complex data management and airline-specific systems. Our team has identified an approach to aviation security that encompasses the passenger experience, airport environment and the underlying infrastructure. Today's testimony covers the passenger experience and portions of the recommended infrastructure.

CURRENT SITUATION

First, we should address the current situation. Industry capacity has been cut by 20 percent, 80,000 employees have been laid off, hundreds of aircraft have been parked and orders for new aircraft delayed or canceled. In order for Americans to get back into the skies, they need to feel better about what's been done to improve airline safety. The good news is with sufficient assurances of safety and service, pent-up demand could quickly out-pace recent capacity cuts and we can return the air traffic to levels that we saw before September 11th. To achieve this, we must improve existing physical security enhancements with a balanced approach of innovative processes and proven technologies.

To date, priority has been given to physical security measures such as National Guard troops in airport terminals and more rigorous searches at checkpoints and gates. These visible measures appear to be improving passenger confidence. However, these advances in passenger confidence have been offset by declines in cus-

tomer service and convenience. The traveling public has been very patient with increasingly intrusive and time-consuming searches, but they are starting to complain about pat downs and even requirements to unbutton clothing in gate areas. Clearly, this is not a system that is viable long-term.

To stimulate air traffic nearer to pre-tragedy volumes, we must simultaneously address confidence and convenience. The Aviation and Transportation Security Bill references solutions that help us accomplish these objectives. Among other things, the bill calls for trusted passenger programs, improved baggage management processes and enhanced passenger pre-screening systems.

We fully support these initiatives because they address the fundamental security questions:

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

They also leverage proven technologies and can be rolled out quickly.

ARE THEY WHO THEY SAY THEY ARE?

In a new era of suicide terrorists, positive identification of passengers is as important as the detection of bombs and weapons. Currently, traditional identification documents, like drivers licenses or passports, are the only means of validating the identity of passengers, yet these documents are easily stolen or forged. Recognizing this, we now have to treat all passengers as "high-risk". This means more random searches, more inconvenience for law-abiding citizens and, perhaps worst of all, more wasted time for security personnel who should be focused on truly high-risk passengers.

EDS joins other industry partners and other aviation associations in recommending an "opt-in" process to increase the number of "known" or "trusted" 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. And third, it increases security for all because security resources can be focused on a smaller universe of "unknowns".

The cornerstone of the trusted traveler program is voluntary biometric identity systems. These systems could be used to speed the check-in process for frequent travelers, which represent as much as 50 percent of the flying public. Having once registered with a system where full proof of identity was provided and background investigation successfully completed, a traveler, would be issued a smart card. With this card, the passenger can authenticate his or her identity in seconds at a biometric checkpoint, using viable biometric technologies such as fingerprint scanning, hand geometry, or facial recognition.

EDS has such a system in place today at Ben Gurion International Airport in Israel which is considered the safest airport in the world. It allows registered Israeli citizens to authenticate their identities with magnetic card and biometrics technologies, saving 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 Computer Aided Passenger Pre-Screening System (CAPPS) is a great start, regulators, airlines, unions and associations agree that improvements are warranted. EDS recommends a centralized passenger evaluation system that will objectively evaluate the level of risk that each individual pose to the transportation system. With a centralized system, risk criteria could be changed near real-time and could instantaneously alert all airlines of potential threats. Further, this system would be the foundation for the comparison of passengers to law enforcement watch lists.

This kind of system is not new. In fact, EDS is currently operating a similar prescreening system for a number of U.S. airlines—processing approximately 70 million passengers annually. Given that a number of airlines already utilize this system, EDS feels that this version of CAPPS is the logical foundation of a national passenger evaluation capability and could be deployed in 6 to 9 months depending on final requirements and funding arrangements.

EDS also recommends a Flight Risk Management Solution that aggregates individual risks into an overall flight or airport risk situation. This solution would provide airports with information on when to escalate security measures.

ARE THEY CARRYING ANYTHING ILLEGAL?

As the Aviation Transportation and Security Act requires, all checked baggage should be screened using explosive detection equipment. However, even after 100 percent screening is achieved, systems must be implemented which ensure the integrity of the baggage.

Once a bag has been cleared of explosive materials, it needs to be secured—either by sealing the bag itself or sealing it within a luggage container. After being sealed, the bags or containers could be tagged and tracked throughout the airport using bar code or radio frequency identification devices (RFID's like toll tags on highways). Using this technology, airport and airline 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 also facilitates the positive matching of baggage to those actually boarding an aircraft and allows personnel to quickly locate and remove the unattended checked baggage. This same system could be used to secure and monitor cargo and mail.

A number of baggage identification, sortation and reconciliation systems are in place today, both here in the U.S. and around the world. Many rely on bar code technology, although RFID baggage systems are being piloted at several airlines today. Further, RFID is a proven technology frequently used in other industries—especially to assist in tracking and monitoring vehicles, inventories and managing supply chains.

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. It is imperative that a solution to aviation security be approached from an enterprise perspective. Such an information system will have to process data real-time and must be accessible 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 hundreds of thousands of biometrically enabled smart cards for the U.S. Department of Defense. EDS prescreens millions of passengers using its client-server CAPPS system every year. Israel's Ben Gurion Airport utilizes a biometric system to expedite immigration 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 data bases 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.

IN CONCLUSION

The challenge is to restore confidence and convenience at the same time. Logic dictates that restoring one without the other will not solve the problems we face. The solutions I've described today would compliment physical security enhancements and compensate for the negative impacts on service. By implementing these solutions, we will restore the confidence of the flying public and get Americans back in the skies again.

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

Senator CLELAND. Thank you very much, Mr. Planton. I was just sitting here thinking, it is fascinating what is evolving out of our effort to, as Michael Jackson said, balance world class security with world class convenience and customer service.

The 15 percent at Ben Gurion——

Mr. PLANTON. Yes.

Senator CLELAND [continuing]. Choose, shall we call it for want of a better term, the trusted passenger route. If we had such a system in America, what is your guess of how many people would voluntarily sign up?

The reason I ask that, I fly, you know, every Friday and every Monday to come back here and I fly all the time. And I see a lot of the same people on the flight. I mean there are a lot of business travelers out there. These are not first time flyers; these are frequent flyers.

I cannot help but think that maybe that number might be higher in the United States. What is your guess?

Mr. PLANTON. As I stated, frequent flyers for some airlines account up to 50 percent of their passengers. I would believe that the United States, Americans, would opt in for convenience sake. That benefits us two-fold. It moves frequent travelers, yourself, through security, but also shortens the line for non-frequent travelers like the individuals taking that once in a lifetime vacation who have never flown before—that shortens that line, and we have seen that at the Israeli Ben Gurion Airport. We have also seen that at our immigartion checkpoints along the Mexican border with some of the systems that we piloted with the INS.

Senator CLELAND. Thank you. And it seems too with our web technology and so forth, that for a lot of people, getting a reservation over the web if there would be a way to preapply for something like that and do a lot of the checks and so forth even for the non-frequent flyer. I do not know. I think we are getting into a fascinating world where our telecommunications, our data bases, our intelligence capabilities and so forth can, as the gentleman said, Mr. Selvaggio, focus more and more on the passenger rather than on who has tweezers and who has a stitching needle.

One final question and we will wrap it up—oh, actually our two guests here, Colonel Brooks and Richard Duncan, since you are really the people in charge of security here, you ought to be allowed to make a statement here. Mr. Duncan, do you want to go first, if you care to say anything?

STATEMENT OF RICHARD DUNCAN, HARTSFIELD INTERNATIONAL AIRPORT

Mr. DUNCAN. Thank you for allowing me to speak. I believe Mr. DeCosta has really stated the position for Hartsfield. However, I personally would like to thank you for taking the lead on the aviation security and especially for drafting the legislation for prosecuting those who violate security. As a security manager, I constantly have to work with the policies and procedures, but when we have a violation and there is nothing to fall back on for that particular individual, it really is disheartening for the staff to work with.

We are constantly looking at our procedures and trying to make sure that we are providing the quality services while maintaining security that everyone expects of us.

Thank you.

Senator CLELAND. Thank you, Mr. Duncan.

Colonel Brooks, is it?

STATEMENT OF COLONEL BROOKS, ATLANTA POLICE DEPARTMENT

Colonel BROOKS. Senator Cleland, thank you for inviting——

Senator CLELAND. And you are with the APD, Atlanta Police Department.

Colonel BROOKS. Yes, sir, I am with the Atlanta Police Department. I am the Precinct Commander at Hartsfield.

I just wanted to assure you that I have met with Mr. Keith Varner, the Solicitor General at Clayton County, last week and we are aggressively pursuing criminal charges against the individual who breached our security. So we are pursuing State charges on that, but it would certainly help if there was something on the Federal level that we could pursue also.

Senator CLELAND. Thank you very much. I intend to introduce that legislation this afternoon.

Wrapping it up, let me just thank you all. But one final question—a year from now, if we meet together again in December of 2002, is it your opinion that we will be presiding over a much—not only a much improved aviation security system, but really a superior security system to that basically it is available around the world?

Colonel Brooks, you want to take a stab at that? Yes or no.

Colonel BROOKS. Since September 11, we have seen a vast improvement in security systems and law enforcement at Hartsfield—I can speak for Hartsfield. I think a year from now, we are going to see an entirely different aviation industry, security just being a part of that. And I think we will see a vast improvement in that timeframe.

Senator CLELAND. Mr. Duncan.

Mr. DUNCAN. I concur that we will see major improvements within the systems and I think everyone really would have to start thinking a little bit differently from what we think about airport security because when we think of airport security, we think only of the checkpoint, but there are a lot of other layers of security that we have been dealing with in trying to assure that everyone understands those things that are associated with it. From the parking lot all the way to the aircraft, we are building layers of security and reinforcing security throughout the airport.

Senator CLELAND. Thank you.

Mr. DeCosta.

Mr. DECOSTA. I echo the sentiments of my colleagues. I think that with the attention that is being given to this nationwide from Congress, Federal agencies and every airport manager in the country are focused on security in a much different way now, as compared to before. Our commitment to meet the challenge will make sure that we have the safest system in the entire world.

Senator CLELAND. Thank you.

Mr. Selvaggio.

Mr. SELVAGGIO. I can say that every airline executive is also committed to security in a way that we have never even thought of before. So the commitment from airline executives is universal and I think yes, it will be better a year from now and I think a key is technology and it is technology that we have seen in evaluating the customer that would like to move to a trusted passenger

program and it is also the technology that we are going to deploy in examining and screening baggage.

Senator CLELAND. Thank you very much.

Mr. Kalil.

Mr. KALIL. Yes, sir, I believe this industry will be—a year from today will certainly be more focused on security than it ever was in the past. I do agree we have to marry that enhanced security with enhanced customer service and I think the trusted customer concept is the way to go. One of the things that we have tried to do is instill that sensitivity for security down to every single employee in the company because it is the people on the front lines that really ensure that our security is what it should be.

Senator CLELAND. Thank you very much, sir.

Dr. Bevan.

Dr. BEVAN. Yes, I think there are a number of technologies, commercial off-the-shelf technologies that could help us in the next year. Beyond that, I am a little concerned that there are technologies that are available that will not get developed and we will need them to continue to improve our security and improve the system as we go along. In other words, we should not, after a year, rest on our laurels and say it is all over with. This is a long-term kind of struggle and I am sure there are other technological improvements that could help.

Senator CLELAND. Thank you very much.

Mr. Macginnis.

Mr. MACGINNIS. Senator, we thank you and you are the leader in this industry right now, we applaud you once again for taking the initiative and introducing this bill so we do have some security measures to start with. We pledge the support of the Air Line Pilots Association in helping you.

Senator CLELAND. Thank you very much, sir.

Mr. Planton.

Mr. PLANTON. Thank you for your time today. I do believe we will have a secure national airspace system a year from now. We will see our Federal workforce trained and implemented, and my job in EDS is to take what we know now and apply it to the airline system and leverage that across the United States. Thank you.

Senator CLELAND. Thank you all very much. And of course all of this is designed to enhance the confidence and security of the American public in flying again in not only the numbers we saw before September 11, but in greater numbers.

Thank you all very much. Let me just say that the wonderful staff on this Committee deserve the credit for putting this together. I would like to thank my associate, Jane Terry, and her wonderful work with the Commerce Committee; Sam Whitehorn, Gael Sullivan and Mike Reynolds for being with us today.

We will call the Committee to an end. Thank you very much.

[Whereupon, the Committee was adjourned at 12:26 p.m.]

○