THE FUTURE OF TSA'S REGISTERED TRAVELER PROGRAM

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRSTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

NOVEMBER 3, 2005

Serial No. 109–54

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
35–694 PDF WASHINGTON : 2007

COMMITTEE ON HOMELAND SECURITY

Peter T. King, New York, *Chairman*

Don Young, Alaska
Lamar S. Smith, Texas
Curt Weldon, Pennsylvania
Christopher Shays, Connecticut
John Linder, Georgia
Mark E. Souder, Indiana
Tom Davis, Virginia
Daniel E. Lungren, California
Jim Gibbons, Nevada
Rob Simmons, Connecticut
Mike Rogers, Alabama
Stevan Pearce, New Mexico
Katherine Harris, Florida
Bobby Jindal, Louisiana
Dave G. Reichert, Washington
Michael McCaul, Texas
Charlie Dent, Pennsylvania
Ginny Brown-Waite, Florida

Bennie G. Thompson, Mississippi
Loretta Sanchez, California
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Jane Harman, California
Peter A. DeFazio, Oregon
Nita M. Lowey, New York
Eleanor Holmes Norton, District of Columbia
Zoe Lofgren, California
Sheila Jackson-Lee, Texas
Bill Pascrell, Jr., New Jersey
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida

Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity

Daniel E. Lungren, California, *Chairman*

Don Young, Alaska
Lamar S. Smith, Texas
John Linder, Georgia
Mark E. Souder, Indiana
Mike Rogers, Alabama
Stevan Pearce, New Mexico
Katherine Harris, Florida
Bobby Jindal, Louisiana
Peter T. King, New York *(Ex Officio)*

Loretta Sanchez, California
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Peter A. DeFazio, Oregon
Zoe Lofgren, California
Sheila Jackson-Lee, Texas
James R. Langevin, Rhode Island
Bennie G. Thompson, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

WITNESSES

PANEL I

PANEL II

FOR THE RECORD

THE FUTURE OF TSA'S REGISTERED TRAVELER PROGRAM

Thursday, November 3, 2005

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Economic Security,
Infrastructure Protection, and Cybersecurity,
Washington, DC.

The subcommittee met, pursuant to call, at 12:16 p.m., in Room 311, Cannon House Office Building, Hon. Daniel Lungren [chairman of the subcommittee] presiding.

Present: Representatives Lungren, Rogers, Dicks, DeFazio, Langevin, and Thompson.

Mr. Lungren. [Presiding.] The Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity will come to order.

The subcommittee is meeting today to continue its oversight of the Registered Traveler program and to assess what measures are needed to move it beyond its pilot phase to a truly nationwide system.

I would like to welcome everybody to today's hearing. We have already met twice this year on the prospect of a Registered Traveler, or, as I prefer to call it, a trusted traveler program, being rolled out at our nation's airport. Some may wonder why a third hearing is necessary.

Well, it is my belief that the successful implementation of an interoperable program for voluntary enrollment of frequent fliers will not only help focus TSA resources towards those passengers that perhaps pose the greatest risk, we will also reduce the burden and hassle often associated with air travel.

I am reminded that, four weeks ago, my wife purchased an airline ticket to travel from Washington, D.C., to our home in Sacramento. This week, she intended to depart from Reagan National Airport, catch a connecting flight at Dallas-Fort Worth, and then arrive at Sacramento, California.

On the day of her flight, she received a call to inform her from the airline that a storm in Dallas-Fort Worth had caused her flight to be cancelled.

But she was told not to worry. They could get her booked on another ticket. It would be on another airline. Instead of going through Dallas-Fort Worth, she would go through Phoenix.

Well, that was all fine. But imagine her frustration when she arrived at National and then was immediately selected for secondary screening. She was misidentified as a threat.

And I know we have various matrix, but she is a frequent flier. I would like to assume that she may also be considered a trusted traveler. She purchased her ticket well in advance and did exactly as the airlines instructed.

The airlines knew she had been diverted from her original plans. She knew it. Unfortunately, the way the system works, TSA did not recognize it. So time and resources were spent on going through her belongings and physically searching her unnecessarily.

I mean, these are the kind of frustrations that I think people see on a regular basis. And I have said at other times that the most regular exposure that the average citizen has to DHS—and, in some cases these days, the federal government—is when they are going through a TSA line at the airport. And that very much forms their opinion about how the federal government operates these days.

I think this was an inconvenience that much of the traveling public experiences. It is also a drain on precious TSA resources and, in my judgment, an inefficient way to conduct homeland security operations at our nation's airports.

As we all know, frequent fliers disproportionately represent the traveling public. It is my understanding that if only 5 percent of travelers registered for the Registered Traveler program, it is probable that they would represent 25 percent of the traveling public on any given day.

For TSA, this would mean that that haystack that many of us have referred to, from which you attempt to identify passengers that may pose a problem, could be decreased by one quarter.

I have heard from the TSA twice on why they cannot roll out this program now. Today, I hope to hear why they can.

The private sector represented here today in the second panel has told me that they have the capability to roll out a fully operational and interoperable Registered Traveler program at 50 of the nation's largest airports within a 60-day time span. And we will have an opportunity for them to say that here and for us to question as to whether that is actual and real.

I would like to receive an authoritative and clear answer from our administrator here today as to why TSA has taken so long to implement the program and, hopefully, how they plan to implement it in the near future.

I would also like to explore the benefits that may come from allowing the private sector to operate the Registered Traveler program, as currently being done, for instance, at Orlando Airport.

I believe that all—all passengers—may benefit from the investment of private-sector resources in the screening technology for airports.

I would like to thank our witnesses for taking the time to join us today. I look forward to hearing each of your perspectives on this issue.

It is now my pleasure to recognize the ranking member of the full committee, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you, Chairman Lungren.

It is good to see you here, Mr. Administrator.

It has been just over 4 months since the committee held its last hearing on the Registered Traveler program. A lot has happened, to say the least, since that time, and we would like to hear from you, with respect to that.

Phase two of the Registered Traveler pilot, a public-private partnership, administered by Verified Identity Pass, Lockheed Martin, and the greater Orlando Airport authorities, started.

Since it started, 10,000 travelers enrolled in the Orlando pilot. I would like for you to talk a little bit about why, on September 30, TSA summarily cancelled phase one of that program and those individuals we talked about who were then deactivated, had their cards deactivated, had it done so with no notice.

Nearly 60 airports signed on to the Registered Traveler Interoperability Consortium. And the American Association of Airport Executives moved forward with plans to manage the Registered Traveler application.

Yet, Mr. Administrator, a lot has happened since the intervening months.

Many of these changes in the program and TSA raise new questions. The largest one is: Where is TSA going with the Registered Traveler program?

Congress directed TSA in 2002 to establish a known or registered traveler program that allows passengers, who provide their biometric and biographical information, access to expedited security processing at the checkpoints. Over 3 years have passed, and the future of this program is still murky.

The title of this hearing is "The Promise of Registered Traveler." For years, there has been a steady drumbeat from business travelers, air carriers, and ordinary folks for a faster way of getting processed.

People understand the need for thorough screening in a post-9/11 world. However, naturally, they would like the process to be as quick and painless as possible. That is why the interest in the Registered Traveler program is so great.

Again and again, the traveling public has said that they are willing to give up some of their privacy and hand over their biometric information for the opportunity to forego secondary screening and access to a special lane.

From a security perspective, the opportunity to reduce the haystack and separate the known from unknown travelers makes a lot of sense, given our limited resources.

At present, registered travelers still undergo the same physical screening as all the other passengers receive. However, I am interested to learn whether or not TSA is considering allowing those travelers to keep their coats and shoes on at the checkpoint.

This is an issue that comes up at every hearing. Those of us who go out of Reagan National, we have to take our shoes off. If we ask a question, we get the secondary screening.

[Laughter.]

So I guess you just follow suit and take your shoes off, even though we know there is no regulation that mandates taking your shoes off. It is sort of up to the individuals.

But, nonetheless, I appreciate you being here, Mr. Administrator. And I look forward to your testimony and the testimony of the witnesses in the second panel.

Thank you. I yield back.

Mr. LUNGREN. Other members of the committee are reminded that opening statements may be submitted for the record.

I just might mention that I am involved in a reconciliation markup in the Budget Committee in the hearing room directly below here, so I may have to run down for a vote and then come on back. But Mr. Rogers has indicated that he will more than competently take my place.

We are pleased to have two expert panels of witnesses here today to give testimony on this important topic.

I would just remind the witnesses that their entire written testimony will appear in the record. And we ask that you would limit your oral testimony to a 5-minute period allotted.

The chair now recognizes the honorable Kip Hawley, assistant secretary of the Transportation Security Administration, Department of Homeland Security, to testify.

PREPARED STATEMENT OF THE HONORABLE PETER T. KING

Thank you, Mr. Chairman. Let me first welcome and thank the witnesses for appearing before the Committee today. I commend the Chairman on the timeliness of today's hearing because I believe that it is vitally important that we take another hard look at the status of the Registered Traveler Program.

Congress intended the Registered Traveler Program (RT) to be an important risk-management tool that would effectively reduce the haystack in which TSA looks for terrorists.

It has been more than a year since TSA rolled out its Registered Traveler pilot program. Last month, TSA ended the first phase of the pilot, but has decided to continue to oversee the private-sector Registered Traveler program that was implemented by Verified Identity Pass at Orlando International Airport last July.

In June, TSA testified before this Subcommittee that the RT pilot had "successfully proven the operational feasibility of the Registered Traveler concept, processes, and technologies in a practical environment," and that TSA was analyzing data from the pilot to incorporate best practices into a fully expanded and permanent RT program. Today, we look forward to receiving TSA's report on its findings and recommendations in these critical areas.

Experience to date demonstrates that RT programs can reduce passenger inconvenience while at the same time improving security—by obtaining greater information about certain passengers, and to permit TSA to focus on higher-risk travelers. I am encouraged by data submitted to the Committee indicating that average wait time in line for Orlando's RT members is three minutes, compared with 31.48 minutes for non-RT members.

TSA should have garnered enough experience by now to begin facilitation of a nationwide implementation of Registered Traveler. TSA must move expeditiously to clarify whether Registered Traveler participants will be permitted to keep their jackets and shoes on, as well as whether they would be exempt from secondary screening. TSA must also resolve issues that will enable Registered Travelers to access RT services at other airports.

TSA must address these issues in order for the Registered Traveler program to reach its full potential. However, it also is imperative that TSA ensure that non-Registered Traveler participants are not subjected to longer lines than would otherwise be the case absent a dedicated RT line.

And no matter which RT model or models TSA chooses to pursue, the Federal government must retain its role with respect to setting privacy and security standards.

We have assembled two expert panels today, and I look forward to hearing from the witnesses how we can work together to make Registered Traveler a permanent and nationwide program that enhances aviation security and supports the national economy by encouraging greater aviation travel.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE

Mr. Chairman, I would like to first thank you for holding this hearing today, which is the third on the subject. I would also like to thank our distinguished panel of witnesses for being here. The subject of Registered Travelers is very important, and deserves our utmost attention and consideration. The registered traveler program, if implemented in a safe and effective manner, could greatly help improve the quality of air travel in this country, and relieve burden from our security personnel's strained workload. The Registered Traveler program grants access to separate, shorter security lines at airports to frequent flyers that have passed criminal background checks by federal law enforcement officials. This group of travelers, who take about one-half of all flights in the United States every year, are assured they will not have to endure pat-owns and delays caused by being forced to remove their shoes and laptop computers for additional scrutiny. The federal government's test program has been criticized not for fostering a perception of giving small classes of people special treatment. This is a short sighted view of the program. The Registered Traveler program a benefit to the business travelers, and it.

Mr. Chairman, I would again like to thank you for holding this hearing. I believe with continued work, this program will eventually become a mainstay in airports around the nation. I yeild back the remainder of my time.

STATEMENT OF THE HONORABLE KIP HAWLEY

Mr. HAWLEY. Good afternoon, Chairman Lungren, Congressman Thompson, members of the committee. Thank you for this opportunity to speak about the Registered Traveler program. As you know, TSA is pursuing a security strategy based on the results of Secretary Chertoff's second-stage review.

Key to our strategy are four principles: one, making investment and operational decisions based on risk; two, denying terrorists an advantage based on our predictability; three, focusing on the terrorist, not only the means by which a terrorist carries out a threat; and, four, building and taking advantage of security networks.

In combination with other activities, I believe the Registered Traveler concept can be a valuable piece of our overall security program.

Conducting security checks on Registered Traveler participants as part of their registration can help free up TSA's screener resources to focus on higher risks.

Of course, an element of randomness, with regard to secondary screening, will still be required in order to maintain uncertainty among terrorists who may wish to corrupt the program. I believe Registered Traveler, when combined with other changes, can also make air travel easier for the traveling public.

As you know, TSA's initial five Registered Traveler pilots ended in September 2005. A sub-pilot at Orlando International Airport testing the feasibility of a public-private partnership model is still in operation.

An independent evaluation of the completed pilots has concluded that the Registered Traveler concept is, indeed, viable. The biometric identity verification technology used in the pilots performed accurately and rapidly under airport conditions.

In addition, in comparing the use of smart card technology, versus a cardless option, the evaluation concluded that smart card technology would enhance the security, efficiency and technical capacity of the system.

The evaluation also found that people who participated in the program had a positive impression, found it easy to use, and supported its continuation.

Furthermore, based on the results of the Orlando sub-pilot thus far, we have concluded that the public will accept the involvement of a private company that collects and processes biographic and biometric data. And that, although the fee charged in the Orlando sub-pilot does not cover all the costs of the program, a fee-based program can attract participants.

In keeping with congressional direction and consistent with the results of the programs, we have established an operational framework for the future of the Registered Traveler program.

Interoperability is essential. All registered travelers must be able to access the program at any airport with a Registered Traveler checkpoint.

The program will be able to accommodate all eligible enrollees, using technology that incorporates biometrics. The program will include an element of random security checks, in order to deter terrorist attempts to compromise the program. And the program will protect the privacy of participants.

The program will be funded by fees. I want to thank the Congress for granting DHS the authority to set and collect Registered Traveler fees.

In order to make fully informed decisions, particularly with regard to the business model of the program, TSA intends to offer an opportunity for public comment to solicit additional ideas and recommendations.

In short, TSA is committed to a risk-based approach to passenger screening. And we look forward to working with our stakeholder partners in the private sector as we move to the implementation phase for the Registered Traveler.

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

[The statement of Mr. Hawley follows:]

PREPARED STATEMENT OF THE HONORABLE KIP HAWLEY

Good afternoon Chairman Lungren, Congresswoman Sanchez, and members of the Subcommittee. Thank you for this opportunity to speak with you about the progress we are making with our domestic Registered Traveler (RT) Program since testifying on this matter last June, and discuss the program in the context of Secretary Chertoff's risk-based strategy.

The Aviation and Transportation Security Act (ATSA), P.L. 107–71, directed TSA to explore options for expedited travel at airports commensurate with having information that a traveler does not pose nor is suspected of posing a known threat. In the simplest of terms, the Registered Traveler Program concept is to conduct more extensive threat screening in advance of travel on individuals who choose to participate in the program, and to provide those who are accepted into the program with expedited screening at the airport.

Adapting to a Changing Threat Environment

Created in the aftermath of the 9/11 terrorist attacks, the Transportation Security Administration continues to pursue its vital mission of protecting our Nation's transportation systems. Fundamentally, our challenge is to protect passengers, freight, and our transportation network in a constantly changing threat environment. We know that terrorists will not only look for weaknesses in our transportation system and its security measures, but they will also adapt to perceived security measures. Our approach to security in every transportation sector, including aviation, therefore, must be based on flexibility and adaptability.

TSA is pursuing a security strategy based on Secretary Chertoff's Second Stage Review, the National Strategy for Transportation Security, and the following four operating principles:

First, we will use risk/value analysis to make investment and operational decisions. That means that we will assess risks based not only on threat and vulnerability, but on the potential consequences of a particular threat to people, transportation assets, and the economy. Further, we will assess and undertake risk management and risk mitigation measures based on their effect on total transportation network risk. This holistic approach to risk assessment and risk mitigation may lead us, for example, to redirect the actions of our airport screeners to focus less on identifying and removing less threatening items from carry-on luggage, so that their time and attention can be spent on identifying potential components of an improvised explosive device.

Second, we will avoid giving terrorists or potential terrorists an advantage based on our predictability. TSA will deploy resources—whether they are canine teams, screeners, air marshals, or inspectors—and establish protocols flexibly based on risk, so that terrorists cannot use the predictability of security measures to their advantage in planning or carrying out a threat. This may mean changing or adding to inspection routines on a daily or hourly basis to introduce uncertainty into terrorist planning efforts.

Third, we will continue to intervene early based on intelligence, and focus our security measures on the terrorist, as well as the means for carrying out the threat. Enhancing and expanding the techniques to identify suspicious persons or to detect explosive devices at screener checkpoints is necessary. However, the strongest defense posture detects the terrorist well before the attempt to launch an attack has begun. A coordinated interagency intelligence collection and analysis effort must stand as the first line of defense. Effective dissemination of timely intelligence products to those who need them is a vital component of this effort.

And, finally, we will build and take advantage of security networks. As you may know, I am pursuing a restructuring of TSA that will put a renewed emphasis on building information sharing networks in every transportation sector—rail, transit, maritime, and trucking, as well as aviation. Not only will we work more closely with stakeholders in these industries, we will put a renewed emphasis on sharing intelligence, capacity, and technology with other law enforcement, intelligence gathering and security agencies at every level of government.

Application of Key Principles to a Registered Traveler Program

The relevance and importance of these operational principles are key factors in the development of our plans to institute a nationally available Registered Traveler Program.

In particular, we believe that an effective Registered Traveler Program can and will:

- Provide a significantly higher level of assurance that people in the program do not have terrorist intentions;
- Allow TSA to focus its screener resources on passengers that present a potentially higher risk;
- Retain an element of randomness with regard to secondary screening in order to maintain uncertainty among terrorists who may attempt to thwart the program;
- Protect the privacy of individuals who participate in the program; and
- Make air travel easier for domestic passengers.

Registered Traveler Pilot Programs

Registered Traveler Pilot Programs were initiated in five airports on a staggered basis during the summer of 2004. In partnership with Northwest Airlines, United Airlines, Continental, and American Airlines, TSA established pilot programs at Minneapolis-St. Paul (MSP), Los Angeles (LAX), Houston Intercontinental (IAH), Boston (BOS) and Washington, DC (DCA). Each of the five pilot programs enrolled approximately 2,000 people, who were invited to participate by the airlines from among their "very frequent" fliers. Participation was limited to U.S. citizens, U.S. nationals, and permanent legal residents of the U.S. Participation in the program was entirely voluntary. Participants in these five initial pilot programs were not charged a fee.

Participating passengers provided personal biographic (name, address, phone number, date of birth, and in some locations, social security number) and biometric (fingerprint and/or iris scan) information, as well as government-issued identification (passport or driver's license). Maintaining this information in the database allows continuous screening of the travelers as those databases are updated. The validity of the document was verified using electronic document scanners. The biographic information was used to perform a name-based check against a consolidated terrorist screening database. When a participant initiated travel at his/her home airport, his identity and threat status was confirmed using biometric readers at special kiosks located near the TSA security checkpoint. After identity verification at the biometric kiosk, participants went through normal primary TSA screening, but were not subject to random secondary screening. However, if a program participant caused the walk-through metal detector to alarm or an x-ray of his carry-on items indicated the possible presence of prohibited items, additional screening was conducted. Because the pilot programs were designed to test the effectiveness of the technology and operational processes, participants could not be offered the range of expedited screening benefits that might be available under a fully-validated Registered Traveler program. It was critical to ensure that security was not compromised under the pilot programs.

The initial five pilots ended in September 2005. In June 2005, TSA initiated a sub-pilot program at Orlando International Airport (MCO). Consistent with our goal of engaging the private sector in the work of TSA, this sub-pilot (known as the Private Sector Known Traveler Program) is intended to test the feasibility and advantages and disadvantages of using a public-private partnership model for the program. In addition, the sub-pilot is testing whether people are willing to pay a fee to participate in such a program. Under the Orlando sub-pilot, participants pay a fee of $80. The Orlando sub-pilot is expected to continue past January under the terms agreed to by the Greater Orlando Airport Authority and TSA, and to merge with a nationwide Registered Traveler Program when practical.

Lessons Learned Thus Far

An independent evaluation of the five initial pilot programs was conducted by PMA/Booz Allen Hamilton. The evaluation concluded that the Register Traveler concept is viable.

The biometric identity verification technology performed accurately and rapidly under airport conditions. Biometric verification took, on average, approximately 10 seconds. With the use of dual biometrics (fingerprints and iris scan) identification verification was successful 99 percent of the time, a significantly higher success rate than achieved using fingerprints alone. The pilot programs also tested the use of smart card technology versus a card-less option, and concluded that smart card technology would enhance the security, efficiency and technical capacity of the system.

In addition, participants had an overwhelmingly positive impression of the program, and a desire to see the program continued and expanded. Ninety-five percent of the participants surveyed indicated that the system was easy to use; ninety-eight percent supported its continuation. Further, based on the results of the Orlando sub-pilot, we have concluded that the public will accept the involvement of a private company in a Registered Traveler Program that collects and processes biographic and biometric data, and that a fee-based program can attract participants. The elasticity of the fee structure (i.e., the extent to specific fee amount affects enrollment decisions) could not be tested under this model.

Next Steps

TSA is pleased with the results of the five pilot programs that have concluded and look forward to the results of the sub-pilot that is still underway. We are committed to the development of a Registered Traveler Program that will enhance aviation security, ease travel for passengers, and permit TSA to better focus security resources based on risk.

In keeping with Congressional direction and consistent with the results of the pilot and sub-pilot programs, we have established the following operational framework for the Registered Traveler Program:

- **TSA will establish the requirements** for a security background check and the biometric standards for the program, and will certify participating vendors.
- Program participants will receive **benefits commensurate with the background check** that is performed.
- The program will provide for **interoperability** at all Registered Traveler sites from the onset of operations. This means that a Registered Traveler participant must be able to access the program at any airport with a Registered Traveler-enabled checkpoint lane.
- The program will be able to accommodate all eligible enrollees through the use of technology that **incorporates biometrics.**
- The program will use a **public-private partnership model** with a clear delineation of responsibilities, and will take advantage of the private sector's ability to adapt operations to meet customer expectations and make rapid capital investment decisions.
- The program will define the role of the **Transportation Security Clearinghouse.**
- The program will include an element of **random security checks in** order to deter terrorist attempts to compromise the program.
- The program will be fully **funded by fees.**
- The program will **protect the privacy** of participants.

Let me briefly describe a few significant issues that we are currently working to resolve.

Interoperability. Interoperability is defined as creating a biometric system in which the act of verification at any airport draws the same result regardless of the specific hardware and software used at the individual airport. Standards are still evolving for the biometric industry so the challenge will be in defining a system requirement to allow for interoperability while maintaining a level field for competition among manufacturers. In order to ensure that program participants can access the Registered Traveler Program benefits offered at any participating airport, TSA must develop and promulgate technical and policy guidelines prior to program launch. TSA is working with experts throughout DHS, as well as international industry leaders, to ensure that these requirements are fully identified and clearly defined. In addition, we are working with other DHS agencies to determine where systems, equipment and database sharing might be feasible, with a view toward potential future integration with various international travel facilitation programs managed by U.S. Customs and Border Protection (CBP) and the U.S. VISIT Program.

Roles and Responsibilities. TSA is committed to maximizing private sector involvement in the operations of the Registered Traveler Program without compromising security requirements. Potential opportunities for private sector involvement include participant recruitment and marketing, participant enrollment, identity verification at the airport, and vendor qualification verification. TSA is currently working to clearly define these opportunities and the qualifications required to perform these tasks, as well as the legal and contractual agreements required to establish and maintain these relationships. In addition, we are working to appropriately define the roles and responsibilities of the Transportation Security Clearinghouse, and to establish the business processes and technological requirements to meet these requirements.

Passenger Benefits. TSA is currently examining the full range of potential benefits that can be offered to Registered Traveler participants, consistent with risk-based high standards of security. These options range from exempting participants from some current screening requirements, such as the removal of coats and shoes, to providing separate dedicated screening lanes to Registered Travelers as volume permits. To the extent possible, TSA believes that benefits should be consistent across airport environments. However, our ability to provide benefits such as dedicated screening lanes will be limited by the design and space availability at participating airports. In addition, TSA is strongly considering whether a full criminal history records check should be undertaken. We would anticipate that a full criminal records check, when done in conjunction with our collected biometrics, would allow us to better screen applicants to the program and provide them with more significant benefits. In sum, an analysis of both the effect on risk and the feasibility of each potential benefit is necessary prior to establishing a baseline set of benefits that can be guaranteed to program participants.

Program Fees. The establishment of program fees is closely linked to program benefit decisions. People will make decisions regarding enrollment based on both the cost of program participation and the benefits offered. A key premise of the program will be that it is funded entirely through fees. I want to acknowledge and thank Congress for granting DHS the authority to set and collect Registered Traveler fees.

Compatibility. TSA is also examining whether and how to integrate individuals who have security clearances through other programs, as well as whether and how the program can be made compatible with other domestic and international trusted traveler initiatives.

In addition to the factors already discussed, it will also be necessary for TSA to work with the airports to incorporate RT requirements as amendments to their respective Airport Security Plans (ASP). The ASP governs the security measures and responsibilities for an airport. To the extent possible, TSA will provide a template to facilitate this effort. But we also recognize that a degree of customization will be necessary based on the individual security needs at each airport.

In order to make fully informed program decisions, TSA intends to offer an opportunity for public comment to solicit additional ideas and recommendations regarding potential business models and other program elements. We have already informally consulted with stakeholders in the development of these procedures and are eager to move forward as quickly as practical.

As you know, TSA's primary mission is to secure our Nation's transportation systems. The Registered Traveler Pilot Program has demonstrated the viability of using security threat assessments and biometric-based identity verification technology in an airport environment. We believe that a nationwide Registered Traveler program can provide expedited screening for many travelers and enhance aviation security, as well.

Thank you for the opportunity to testify today. We look forward to working with the Subcommittee as we continue our efforts to strengthen homeland security. I will be pleased to answer any questions you may have.

Mr. LUNGREN. Thank you, Mr. Hawley, for your testimony.

At this time, I would like to ask several questions. I will keep myself to 5 minutes and then recognize members, as is customary.

Mr. Hawley, thank you very much for your statement. Both in that and in others conversations I have had with you, I believe you have a commitment to making this thing work.

And so, as part of that commitment, can you give an idea of what the TSA's time frame is for actual implementation of the Registered Traveler program?

Mr. HAWLEY. Yes, sir. We are committed to the Registered Traveler program and that we expect that, by January 20, 2006, TSA will issue guidance to the industry regarding the biometrics, to collect and how to store that information on Registered Traveler cards.

TSA will announce at that time program benefits to Registered Traveler participants. And, from the private sector, we expect to hear by then from interested parties that want to submit comments to TSA on the Registered Traveler economic model.

And then, on April 20th, three more things happen: One, TSA will select an entity to certify service providers and manage their compliance; secondly, TSA will issue amendments to the airport security plans establishing the requirements for airport checkpoints and verification providers; and then, third, the private sector will get back to us and submit a plan to achieve interoperability of the program.

And we expect that, by June 20, 2006, the first Registered Traveler participants will go through the checkpoints.

Mr. LUNGREN. So the specific dates are January 2006 for—

Mr. HAWLEY. It is for us to say what benefits you get for being a registered traveler specifically. Is it you keep your shoes on, you keep your coat on? If there are other benefits, they would be announced at that time.

We will also issue guidance to the industry that says, "This is what we expect by way of the card that you will have to give us and what is required to be on them."

Mr. LUNGREN. And then the second date would be?

Mr. HAWLEY. The 20th. I should have mentioned, on January 20th, that we are expecting the private-sector parties to tell us their business model.

And then the second date is the 20th of April, which is where we will have an entity to go out and check that, in fact, the things that are alleged to have happened on those biometrics and the security background checks actually happened.

And then we will work with the airports to have the security amendments needed to operate new equipment in the airports. And we expect to hear on that date from the industry on the interoperability of their equipment, which then leads us to, we expect by the 20th of June, that passengers should use the system.

Mr. LUNGREN. And, by saying that they would use the system, that presumes that we can do the background checks, and get the information back, and these folks would be registered?

Mr. HAWLEY. Yes, sir.

Mr. LUNGREN. What determination, if any, has been made, regarding what background information will be disqualifying for the applicants? Or has that been yet determined?

Mr. HAWLEY. Has not yet been determined, but the issue of a criminal history background check plays into this equation, in that, if we require that criminal history background check, it would require a rule making, which would extend the period of time in which we would have to implement.

So it would push out the date as much as a year, if we were to require that now. So what we are contemplating is the arrest and warrants check, the terror watch list check, and essentially the information we have done in the pilots.

And then we will consider during the course of the year whether we, in fact, do need the criminal history background check to add to that in a second phase of the program.

Mr. LUNGREN. But, because of rulemaking authority and procedures, that would take a delay, with respect to that aspect of it?

Mr. HAWLEY. Yes, sir. And we did not want to hold the whole program up for that.

Mr. LUNGREN. Do you have already in mind what redress process would be established to handle cases where applicants are denied participation in the program, believe they have been denied improperly, and therefore have a chance to present their case?

Mr. HAWLEY. That would be part of the January 20th deliverable.

Mr. LUNGREN. Okay. Thank you very much.

And the ranking member of the full committee, Mr. Thompson, is recognized.

Mr. THOMPSON. Thank you very much.

Thank you for your testimony, Mr. Hawley.

Once the program is fully implemented, how many passengers are you estimating will be included?

Mr. HAWLEY. It will be a free-market situation. And we will be prepared to adjust our operations to whatever the market dictates, so that we will have an idea, from the number of traveler cards that are submitted, what that volume will be. And then we will be able to adjust accordingly.

But we do foresee an upper limit for the program.

Mr. THOMPSON. Okay, well, let's say the program is highly successful. Do you see this adding an additional cost for screeners or anything?

Mr. HAWLEY. I see that it very well will add some cost to us, which we will seek to recover from the fee authority that I mentioned in my opening statement, that we will prepare an estimate of what those costs will be, and we will have that submitted for consideration in the *Federal Register*.

Mr. THOMPSON. Now, that fee assessment, is that to go to the traveler, the person? In other words, you will divide your cost by the number of travelers?

Mr. HAWLEY. Yes, sir. We expect to have the equivalent of a license fee. So, as I said, per registered traveler, we expect it will be X number of dollars that would come to us and that we anticipate that the private-sector model, obviously, private-sector partners would want to add whatever they put to it, in relationship to the value added they provide.

Mr. THOMPSON. One of the discussions earlier, in an earlier hearing, talked about how people arrived at the cost for the Registered Traveler program. At that time, if my memory serves me correct, we were told that it was not a process of bidding but it was just a negotiated price.

Now, what is your recollection?

Mr. HAWLEY. Our view is that we will figure out what we anticipate the cost is to TSA, the federal taxpayer, of running the program, supporting the program. And that would be the fee that we request.

And then, as we operate ongoing, if we are wrong, then we would come back and make a change.

Mr. THOMPSON. But you do not anticipate recovering anything other than fee for cost?

Mr. HAWLEY. We do not anticipate using this as a supplemental revenue generator for TSA.

Mr. THOMPSON. Have you looked into—well, there was a memo that came out in August that talked about some things that could be included, that you could carry on planes, a knife, for instance. Are you familiar with the memo I have referenced?

Mr. HAWLEY. Yes, sir.

Mr. THOMPSON. Have you all reached some conclusion on the items that could be carried?

Mr. HAWLEY. We are looking at that very actively now. And it fits within the overall framework of the security program we have in place for aviation and for airport passenger operations.

And we are looking at the prohibited items. We are looking at the SOPs, standard operating procedures, that we do there. We are looking at the CAPPS process. We are looking at the Registered Traveler process. And we are looking at Secure Flights, all of those things within one program.

So Registered Traveler is a piece of that program. And the prohibited items list is another piece. But it is important to recognize that they are all interconnected. And, in a risk management approach, they have to be.

Mr. THOMPSON. So you have not reached a conclusion?

Mr. HAWLEY. Have not reached a conclusion, but we are gathering data and working on it actively.

Mr. THOMPSON. Any idea when you anticipate a conclusion on it?

Mr. HAWLEY. Yes, sir, January 20, 2006.

Mr. THOMPSON. The entire process?

Mr. HAWLEY. For the prohibited items. What we are shooting for, sir, is that, when we know what the Registered Traveler program is going to look like operationally, that we will also know what the other components are, because we want them all to be interconnected. And that is the direction that we are headed.

Mr. THOMPSON. Thank you. I yield back.

Mr. DICKS. Thank you very much, Mr. Chairman.

Mr. Hawley, we understand that you are considering changing of the things that are going to be screened. And there is quite a bit of concern out there, and I wanted to make sure here today that you understood that.

I have a statement of Chris Witkowski, director of the Air Safety Health and Security Department, Association of Flight Attendants, AFL–CIO. And I am going to ask that this letter be put in the record, but I want to read part of it.

> We applaud the TSA's desire to keep up with the evolving terrorist threat but strongly oppose any effort to relax the existing ban on weapons and other dangerous items as part of that process.
>
> In that spirit, we would hope that TSA would recognize that any special benefits accorded to registered travelers should, in no sense, lessen security screening or relax the current prohibition on bringing weapons onboard the aircraft.
>
> For flight attendants, frontline personnel with little or no effective security training or means of self-defense, such weapons could prove fatal. These weapons may not assist in breaking through a flight deck door, but they could definitely lead to the death of flight attendants and passengers.
>
> Furthermore, terrorists know all too well that pilots must open the cockpit door to use the lavatory facilities. And this provides an opportunity for takeover of the cockpit, better facilitated with a knife or other dangerous weapons.
>
> It is well to refer back to the 9/11 Commission report, which found that the records of purchases by the hijackers, as well as evidence discovered at the crash site, primarily the site of Flight 93, indicate that the primary weapon of choice were knives with a blade less than four inches long.
>
> The use of knives was cited on all four flights by flight crew and passengers. Box cutters were specifically indicated only in one report, from Flight 77. A box-cutter-type implement, along with a variety of short-bladed knives, was found at the crash site of Flight 93.
>
> Beyond the terrorist threat posed by weapons onboard the aircraft, these implements also can become safety threats in the hand of passengers who become unruly, often having too much to drink or taking controlled substances.

I think that is a serious consideration. And I have another letter here from a flight attendant who literally had a couple passengers get so drunk on the flight that they were, in essence, a threat to the crew and to the passengers.

So I think we have got to think very carefully here about—you know, I understand that these things will not blow up an airplane. But, you know, these are a threat to the crew of the airplane. And I think it should be very seriously considered before relaxing this, especially because of the concerns of the flight attendants.

And I would like to hear your response to that.

Mr. HAWLEY. Yes, sir. We take those thoughts seriously. And I did have the opportunity to meet with Chris and others. And I have heard from quite a few flight attendants and members of the public.

This is a risk balancing process where, if, in our estimation, in view of the protective measures we have in place today for passenger aircraft, which include, in addition to the screening, the federal air marshals, the hardened cockpit doors, very engaged travelers, and other things, resources that we have, that the explosive challenge at the passenger—to bring an explosive on to a passenger aircraft is a greater overall threat than perhaps other things that are currently on the prohibited items list.

So what we are trying to balance is, if we free up screener resources by doing something directed at a less risky threat and can apply that effort to a more risk threat, that that is how we would make that decision.

But it is not going to be done cavalierly. We do take those—and certainly the 9/11 families, we have had the opportunity to hear from them and certainly respect those thoughts.

It is only that if we can improve the overall risk—or lower the overall risk to the system that we would make changes.

Mr. DICKS. There is going to be a lot of differing opinions on this from differing people. I have had several times where I have forgot—I am a fisherman, and I have brought a knife onboard.

I did not object to that being confiscated because, in my own mind, I still believe that those weapons are a threat to the crew and that, in a situation like this—you know, we have got to look at explosives, but I do not think we should be letting things on the plane that are a threat to the crew.

And I hope you will take that—and, Mr. Chairman, I ask unanimous consent that these two letters be put into the record, without objection.

Mr. ROGERS. [Presiding.] Without objection, they are in the record.

FOR THE RECORD

PREPARED STATEMENT OF CHRIS WITKOWSKI, DIRECTOR, AIR SAFETY, HEALTH AND SECURITY DEPARTMENT, SUBMITTED BY HON. NORMAN D. DICKS

ASSOCIATION OF FLIGHT ATTENDANTS-CWA, AFL–CIO

Thank you for holding this hearing to examine the future of the Registered Traveler program and for the opportunity to comment on this important security issue. The Association of Flight Attendants-CWA, AFL–CIO, represents more than 46,000 flight attendants at 21 U.S. airlines, and our members are keenly interested in maintaining the highest standards of airline security.

It is our strong belief that as this Registered Traveler program takes shape, there can be no relaxation in the high security standards demonstrated as necessary by the horrors of Sept. 11, 2001. Keep in mind that it was flight attendants who were the first to lose their lives on 9–11, and who today remain the first line of defense against any terrorist attack on board an airborne aircraft.

This hearing comes at a time when Kip Hawley, director of the Transportation Security Administration, says the agency is considering potential changes to the list of items that are prohibited onboard aircraft. Mr. Hawley notes that the terrorist threat is shifting to explosives and suggests the screening process should be adjusted to reflect today's threats to civil aviation. recent press reports suggest that as part of this re-evaluation, the agency is considering lifting the current prohibition on dangerous weapons such as knives and other dangerous items. This comes despite continuing recognition by the Department of Homeland Security of the Threat of a 9/11-type attack on passenger aircraft.

We applaud the TSA's desire to keep up with the evolving terrorist threat, but strongly oppose any effort to relax the existing ban on weapons and other dangerous items as part of that process. In that spirit, we would hope the TSA would recognize that any special benefits accorded to Registered Travelers should in no sense lessen security screening or relax the current prohibitions on bringing weapons on board the aircraft.

For flight attendants, front-line personnel with little or no effective security training or means of self defense, such weapons could prove fatal. These weapons may not assist in breaking through a flightdeck door, but they could definitely lead to the deaths of flight attendants and passengers. Furthermore, terrorists know all too well that pilots must open the cockpit door to use the lavatory facilities, and this provides an opportunity for takeover of the cockpit, better facilitated with a knife or other dangerous weapon.

It is well to refer back to the 9/11 Commission Staff Report (8–26–04), which found that: "Records of purchases by the hijackers, as well as evidence discovered at the crash sites (primarily the site of Flight 93) indicate that the primary weapons of choice were knives with a blade less than 4 inches long. The use of knives was cited on all four flights by flight crew and passengers. Box cutters were specifically indicated only in one report, from Flight 77. A box cutter-type implement, along with a variety of short-bladed knives, was found at the crash site of Flight 93."

Beyond the terrorist threat posed by weapons on board the aircraft, these implements also can become safety threats in the hands of passengers who become unruly, often after having too much to drink or taking controlled substances.

We strongly believe [potentially dangerous items have no place in the cabin of an aircraft, and urge the committee to instruct TSA to maintain the ban on small knives and other dangerous weapons currently on the list of prohibited items. If small knives are to be allowed in the interest of reducing the time it takes screeners to remove them from bags, please keep in mind that such a change is unlikely to produce a significant time savings, since screeners will have to spend time determining whether a particular knife would meet some allowable blade size limit that TSA comes up with.

We also ask the committee to help ensure that TSA enforces the security screening limit on the number and size of carry-on bags that has been in place since 9–11. This would reduce the number and size of bags to be scanned and would free up a significant amount of screener time to better focus on detection of explosives. A limit on the number and size of carry-on bags has been supported in the past by the air carriers, partly to reduce late departures and missed passenger connections due to time-consuming stowage and retrieval of excessive and oversized bags by passengers during boarding and deplaning. A specific limit on the size and number of carry-on bags could be enforced by placing a simple template that restricts the height and width of bags to be screened at the security checkpoint. Passengers could be notified of the policy in advance, when they purchase their tickets.

If more screeners still are needed, Congress should lift the cap on the screener workforce to provide the resources necessary to maintain an effective aviation security screening program.

October 28, 2005

Kip Hawley
Director
Transportation Security Administration
TSA-1
Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

Re: Aircraft Security

Dear Mr. Hawley:

I am writing to you in hopes that I can convince you NOT to lift the ban on brining small knives, box cutters and razor blades into the cabins of passenger aircraft. I pray that once you hear my story that you will understand why I have deep concerns about flight safety.

I have been a flight attendant for for almost 19 years now and an incident that happened on September 24 has changed me. I had two individuals on my flight bring their own stash of liquor and proceeded to get intoxicated on our flight. At first they were just annoying, but as the flight progressed they became increasingly hostile. They started throwing objects at passengers, kicking the lavatory door and threatening passengers and crew. One passenger was so stressed, she had a panic attack. Parents moved their little children out of their seats and onto their laps. Fearing that these men would hurt someone, we found an off-duty police officer to sit next to them. The police officer then yelled for help as one of the individuals was now out of control and I jumped up and requested assistance to subdue the man with tough-cuffs.

Most people think of a terrorist as an individual from a well-organized group like Al-Qaeda. However, Mr. Hawley, these were TERRORISTS. They were on my flight, terrorizing my passengers and crew. It was us against them. If these men had the kind of dangerous items that you want to bring back onboard, I can tell you without a doubt that the situation would have turned out gravely different.

The cockpit doors have been enforced and now some pilots are allowed to bring guns, but where does that leave the flight attendants? We have no TSA mandatory self–defense training, no weapons, and now you want to again allow passengers to carry sharp weapons and box cutters into the cabin, as they did on 9/11? I ask you, would you want your family on a flight like the one I had and with passengers with box cutters, razor blades and knives?

I want you to know that I have problems going to sleep at night. I think about this incident in my head over and over again. When it is time for me to work a flight, I feel anxious. I wonder is this the day I am going to have to wrestle someone down to the floor because he or she is under the influence of drugs, alcohol or Al Qaeda? Did they make it past security with a weapon, or did my government, the one I rely on for my safety, help them by relaxing the ban against weapons being hidden and carried into the aircraft by anyone who can buy a ticket.

Please think about what I have written to you. I respectfully ask you to NOT change the carry-on rules so that we flight attendants, as well as passengers, won't be stabbed or slashed by an attacker using these deadly weapons in flight because you allowed him to bring them onboard.

Thank you for your time.

Alisa Arnold

Alisa Arnold
PHL Flight Attendant

Cc: Michael Chertoff
Susan Collins
Joseph I. Lieberman
Judd Gregg
Robert C. Byrd
Peter T.King
Bennie G. Thompson
Harold Rogers
Martin Olav Sabo
Ted Stevens
Daniel K. Inouye
Don Young
James L. Oberstar

Mr. DICKS. Thank you.

Mr. ROGERS. Thank you, Mr. Dicks.

Mr. Hawley, I just have a couple of questions on the Registered Traveler program. Are you going to require airports to be interoperative, in order to participate in the Registered Traveler program?

Mr. HAWLEY. We are going to require that any certified registered traveler program is interoperable, which means that a card issued with a registered traveler approval, is valid at every Registered Traveler checkpoint.

Mr. ROGERS. And how far along do you think we are in that process?

Mr. HAWLEY. I have been told that it is a technical issue that is not a show-stopper. But under the proposal that we are making here today, that we would put that in the hands of the private-sector operators who wish to go forward, have them solve the problem and come to us, as opposed to us trying to solve the problem and then issue it whenever we get that done.

Mr. ROGERS. You also mentioned that TSA will work with airports to amend their security programs once a Registered Traveler program is established. Do you envision TSA working directly with an airline at an airport to establish a R.T. program?

Mr. HAWLEY. We expect to work with whoever the group is that comes in to say, "We want to operate this Registered Traveler program," and specifically for an airport, because, obviously, every checkpoint that we operate is with one of our airport partners. And it would be done in close cooperation with them.

Mr. ROGERS. Okay. That is all I have got.

Mr. DeFazio, do you have any questions?

Mr. DEFAZIO. Yes. Thank you, Mr. Chairman.

First, Mr. Hawley, I want to thank you for your testimony here. And I want to congratulate you on something that was quoted in The Wall-Street Journal, regarding a speech you gave at Geneva, where you said you wanted to free up resources, try to redirect them to prevent explosive attacks. I think we can.

And I congratulate you on that focus. Chairman Mica of the Aviation Subcommittee and I, who were key in the creation of TSA, have felt since the beginning that explosives are a major threat.

In fact, given some of the security measures we have taken, it is much less likely they will try and hijack planes, as opposed to just take them down, because that would destroy the industry, as would a commandeered plane used as a weapon. So that focus is welcome.

Do you think that the equipment that is currently being used by the TSA screeners at the checkpoints is adequate for that threat and the best that we could have, two parts?

Mr. HAWLEY. The technology we have at the checkpoints is effective at detecting explosives. It is part of a system which includes—

Mr. DEFAZIO. But only if you use the trace, right? You are not saying that the basic X-ray machines that we threw out a decade ago here on Capitol Hill are adequate to the task, are you? They were thrown out here a decade ago because they were not.

Mr. HAWLEY. Sure. The system is adequate. And it is a partnership with the machine itself and the operator.

And, in fact, we did have an IED, a live IED, that was disassembled, found by a screener using an X-ray machine.

And we are having very vigorous training to be able to use those machines to find certain aspects of IEDs, that we believe that technology does find extremely effectively, so that to elevate the level of performance from that part of it.

And then the trace is highly effective when we do a trace test on a passenger for finding explosives.

Mr. DEFAZIO. Right. So you do not think that the airports would benefit from the machinery that has been installed in the U.S. Capitol, the White House, the Supreme Court, the Treasury Department, and other federal agencies, which have capabilities of rotating an object without having to say, "Excuse me, sir, I am going to carry your bag back around, interrupt the line, and turn it in a different dimension so we can peer at our dull, 1980s-technology X-ray and see if that threat object is really a threat"?

You do not think we would benefit, both to speed up the lines and find threats, if we had this kind of modern equipment, like we use here? Or should we go back to that cheaper, older equipment and sell this to somebody else?

Mr. HAWLEY. Clearly, the technology that is able to spot a variety of explosives that would be included in a terrorist arsenal today are great.

We are piloting—we announced recently four backscatter tests. And we are deploying the puffers, which is a different trace portal, which is highly effective.

So there is new technology being added. The trick to it is to get the throughput to be able to do as many passengers as you can, which brings up the importance of a registered traveler program to say that you can devote the puffers and the backscatters to people who may present more of a problem.

Mr. DEFAZIO. Nice segue, but back to the backscatters. The throughput is actually much more efficient here at the U.S. Capitol, because they do not have to take the bags, and reinsert them in line, and send them through again in a different dimension.

They can actually—since they have a multidimensional image, they can just rotate the image with a mouse or a key, so that they can see it.

I think that if we had these backscatter machines at the airports, which can do both your traditional threats that Norm has expressed concern about, and a much better job on explosives, that the throughputs would actually be improved.

But I realize that costs a little bit of money and so we will not get into that more.

On the nice segue there, onto trusted traveler. There are two, at least, sort of models out there, maybe three. One would be the government chooses a technology, which, by virtue of being a uniform technology, would be interoperable. You are apparently not going to go that route.

So what you want to use is diverse technologies and diverse vendors who would have to make their technology interoperable, apparently. That is apparently where we are headed.

But then, beyond that, there is a next level of questioning, which is the pricing of the product. As you said, the TSA is not even going to necessarily recapture all of its cost, just a fee.

There is the Orlando model, which is a market-based system, which is—they did a market survey which said, "How much will you pay not to stand in a really interminable line?" And they found that was $89.

Now, if the lines were a little longer at other airports, people might pay $120, you know? It has nothing to do with the cost of the system, a legitimate or reasonable cost-recovery effort by the vendor and, more disturbing, it includes a profit incentive to the airport, who could arguably manipulate the lines to drive more people to buy the card so that they could get a cut from more passengers buying the card.

Does the TSA endorse this Orlando price base, potentially market-gouging, monopolistic model?

[Laughter.]

Mr. HAWLEY. That is why we said that we would like to hear business model proposals by January 20th.

And getting back to Mr. Thompson's question at the beginning, about why we stopped the other pilots was essentially that the business model was not flexible. The program did not seem to be one we wanted to use. So we are asking for input on what the right model is.

Mr. DEFAZIO. Okay. If I could, Mr. Chairman, two other quick questions.

One is, I was a little confused on the discussion of needing additional rulemaking for criminal backgrounds, but we can include arrests. Arrests are very inconclusive documents.

Someone may have been arrested, never charged, been arrested, charged, tried, and acquitted. But, you know, people who are sentenced or incarcerated have a criminal background.

I am confused that we would use an arrest to preclude someone, but we somehow cannot get into the criminal background, which would mean the person who was arrested was subsequently convicted.

Mr. HAWLEY. I believe it is outstanding arrests and warrants, although I have to say I am not exactly sure of all the technicalities.

But the criminal history records check is a very full—it is the SIDA badge-type check, which allows you access to the—

Mr. DEFAZIO. Yes, same background check I have to get a concealed weapons permit, which the FBI provides for $50.

Mr. HAWLEY. And to get that done takes the rulemaking. And so that we did not want to delay the program—

Mr. DEFAZIO. Why would it take a rulemaking?

Mr. HAWLEY. That is an excellent question, sir, and one I have asked. And I am told by reliable sources that that is required.

Mr. DEFAZIO. Well, I think the committee would be interested in trying to expedite that, because I think, you know, getting to criminal backgrounds is kind of the key here, as one indicator of risk.

And then, finally, the last one. I was, I think, concerned by something I heard, which seemed to me—you seemed to imply that there would be a new category of random selectees. I have not been randomly selected for quite some time, since I voluntary remove my belt, and my shoes, and do not question people like Benny does and get them—

[Laughter.]

But you seem to be implying that there would be a required subcategory of random selectees targeted toward trusted travelers, because you are worried about the corruption of the system.

I would suggest that we would want to set up a system that could not be corrupted. And that is a big part of the reason why people, other than the really long lines that the airports might create because they get a cut, would buy these cards, would be to not have to go through the strip search at 6 o'clock in the morning, for a random reason, even though they did not set anything off and there is no problem with them at all.

So I am concerned that you are saying somehow—you are feeling we have got to create a new subcategory of random selection. I mean, if you were saying, "There will still be random selections across the entire universe, which might include those people," that is slightly more acceptable.

But if you are saying, "We are going to create a whole new *quote system* here," that would be tremendously destructive to the whole thrust behind the trusted traveler.

Mr. HAWLEY. There will be random selection for every passenger, including registered travelers.

Mr. DEFAZIO. Okay, that is a departure from past practice and something I think the committee would want to discuss further.

Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman from Oregon.

The chair now recognizes the gentleman from Washington, Mr. Dicks, for some additional questions.

Mr. DICKS. Senator Ted Kennedy and Don Young, for instance, have both been improperly placed on security watch lists. Nor is removal from the watch list a simple matter. Senator Kennedy was only able to correct this error after appealing directly to then–Homeland Security Secretary Tom Ridge.

Now, the vast majority of people affected by watch list errors, needless to say, do not have this option. I mean, what do we do about this? There has got to be a way for a person who has not got a problem to get off this list.

And we had a big hearing on this before. And there were a lot of concerns expressed about this.

Can you give us any hope that there is a better way to deal with this problem?

Mr. HAWLEY. Yes, sir. There is. There is a redress process that is available to all citizens.

And it is a way, when somebody is a close match, to resolve the situation so that there is something different. And a special redress number is given to that individual, which goes on the record and is included when the terrorist watch lists are checked.

It is a component of the check which says, if you have a redress number that matches this, then you, by definition, are not the person who needs to be stopped.

So there are circumstances where one time that happens, because the list does change and includes close matches. But once that does happen, there is a process that is very quick that can get a redress number and get them off that list.

Mr. DICKS. On the trusted traveler program, I can see where there would be some privacy concerns here about the information that is gathered.

How do we assure the citizens that this information will be protected and will not be, you know, disclosed?

Mr. HAWLEY. Part of the approval process that we go through before someone is certified to operate the program is a privacy plan that is acceptable and very strong.

Mr. DICKS. Okay.

Mr. HAWLEY. It is a voluntary program, which is another—

Mr. DICKS. And then, again, what does a person do, if they are turned down for the trusted—this was asked, but I want to hear it again.

If they are turned down for the trusted traveler program, what do they do? Is there a way for them to try to clear up what the reason was for their being denied admittance to the program?

Mr. HAWLEY. There will be a process for that. And that is part of that January 20th deliverable, to figure out what that is.

Mr. DICKS. All right. Thank you, Mr. Chairman.

Mr. ROGERS. Thank you.

I wanted to ask a couple of questions. In his written testimony, Mr. Barclay, who is going to be on our next panel, outlines a role for the Registered Traveler Interoperability Consortium, that includes the establishment of principles and processes by which participating airports may enroll in Registered Traveler, where service providers will transmit application enrollment data to the RTIC Registered Traveler management system, which will transmit the data to TSA.

Mr. Barclay also refers to a memorandum of understanding between RTIC and TSA for these purposes. From his testimony, it appears that it is RTIC, not TSA, that is in charge of the Registered Traveler program.

Has TSA executed a memorandum of understanding with RTIC, or AAAE, to affect the principles and functions described in his testimony?

Mr. HAWLEY. No, sir.

Mr. ROGERS. Can you further describe the Registered Traveler management consortium? Can you tell us a little bit about that?

Mr. HAWLEY. That is a body that is its own body, not connected to TSA.

Mr. ROGERS. Okay. Who owns and controls the RTIC, and what is the entity's relationship with the airline pilots? You don't know?

Mr. HAWLEY. No, sir.

Mr. ROGERS. Thank you very much.

The chair now recognizes the gentleman from Oregon for additional questions.

Mr. DEFAZIO. Thank you, Mr. Chairman.

I would just like to come back, Mr. Administrator, to the question of my concern about giving a cut to the airport on top of the fee that might be charged by a vendor. I mean, does the TSA endorse that model, yes or no?

You said it all depends on who makes what proposal, but, I mean, I think there are tremendous concerns regarding that model.

Mr. HAWLEY. It was a very hard part of our work, was to figure out what to do on the business model. And at the end of the day, we were not comfortable endorsing one particular business model. And, frankly, I am not sure I saw one that I was completely comfortable with.

However, that does not mean that one cannot come forward with one. And so our hope is that the private sector competition will generate a lot of different business models and will generate a lot of options for travelers.

Mr. DEFAZIO. But if, let's say, there was one really big vendor, and that really big vendor has a technology, and they are making a proposal and it has a very high, say, entry cost for other vendors.

Since we are not—I mean, it would be one thing—again, back to the point—if we chose a technology and said, "This is what we want, this kind of interoperability using these biometric standards," now, that would be one thing.

But if a major market-dominant vendor comes in and says, "Well, we have got a great technology here, and, of course, anybody else who wants to can try and replicate it, and we will make our architecture available to them, but the entry costs will be very high," I mean, how is that going to work? How are you going to resolve that?

I mean, you know, theoretically, if we are not going to regulate this and it is not going to be government-based, there has got to be competition. To be competition, there needs to be ease of entry, if you have read—

Mr. HAWLEY. Yes.

Mr. DEFAZIO. —Adam Smith, and David Ricardo, and other people. You know, it is on which we base our radical free trade and other economic theories today. It is not necessarily there.

Mr. HAWLEY. That is what I mean by interoperability, so that if this vendor that you described comes up with a wonderful thing that gets certified, and somebody else is able to come up with a certified program and a card, that card is operable at every checkpoint that there is a Registered Traveler checkpoint, regardless of what membership—

Mr. DEFAZIO. So the burden would be on the dominant, huge dominant—you know, say, based in one of the big DOD contractor companies that says, "We will roll this out everywhere, anywhere, and here is all the equipment, and here is the standard, you accept it"?

But if someone else comes in and says, "Well, we would like to compete, too," that large vendor would have to make their cards interoperable with their systems?

Mr. HAWLEY. Correct. We are not going to be picking these vendors. That is why it is a private-sector program.

We are going to be operating with the airports to, say—the airport, let's say, comes to us and says, "We want to do this program. Here is how we will do it. We will check it out, make sure it works, and make sure that every other Registered Traveler card that is sold will operate on that particular checkpoint."

Mr. DeFazio. Yes, again, I am worried about this incentive to the airports. But by not picking, it does not mean you are not going to thoroughly vet every vendor—

Mr. Hawley. Right.

Mr. DeFazio. —and somehow confirm that it is not, you know, a spin-off of al-Qa'ida in a new profit-making mode here in the United States of America?

Mr. Hawley. Yes, sir. That is the April 20th date. That is the date that we get our certified—

Mr. Dicks. Is it April 1st or April 20th?

Mr. Hawley. April 20th, sir.

[Laughter.]

Mr. DeFazio. Okay. I guess I am just not convinced that this is the best way to go, because you can say there may be a multiplicity of vendors and technologies, there may not.

The airports might get a cut. They might not. You know, if you come, as I do, from one of the underserved, mid-, small-sized airports, it is likely there will be little competition. And someone says, "Oh, God, these people here will pay $500 to get one of these cards," whereas you can get an identical, interoperable card in a competitive environment at some other airport where people are competing for $50.

It just does not seem equitable to have that kind of differential across the system. And you would, apparently, you are going to I do not know. Maybe you can buy a card anywhere from any vendor. Is that the way it is going to work? Or is it going be like the captive, you are trapped at your home airport, whoever-vends-there kind of system?

Mr. Hawley. Not a captive, no captives.

Mr. DeFazio. Okay, so, basically, you can go online, find a vendor anywhere who will do an interoperable card for you. And it does not have anything to do with what airline you fly, what airport you fly out of, where you live, anything like that?

Mr. Hawley. That would be an interesting model, and we would look forward to hearing that coming into us.

Mr. DeFazio. And what sort of decision-making process, when you get these competing business models, will you go through, public comment?

Because you say you have to do a rulemaking just to check background, criminal backgrounds. Are you going to have to go through a rulemaking on—

Mr. Hawley. No.

Mr. DeFazio. No?

Mr. Hawley. We are going to look to get the program up and operating as fast as we can. And we are going to check from the security side and the interoperability side. And beyond that, our goal is to let the innovation begin.

Mr. DeFazio. Well, no offense, Mr. Hawley, to where you work—and I am not questioning your motives—but, I mean, this administration does not have a real good track record at looking at competitive bids and getting the best value for the taxpayer or, in this case, the consumer.

And I am very concerned about something that is so loosely constructed. And hopefully, this committee will exert some oversight on that.

And just on the other issue, I would really like it if your staff could to provide to our staff their technical or legal reasons why they believe, in a voluntary program like this, you need to go through a rulemaking to check criminal backgrounds on people and how we might rectify that, because I really do not believe these cards are going to be that meaningful, if we are not able to check people's criminal backgrounds.

I just think that is a big problem? Thank you.

Mr. ROGERS. The chair now recognizes the ranking member of the full committee, Mr. Thompson, for any questions he may have.

Mr. THOMPSON. Thank you very much.

Going back to a question I asked earlier about the cost—and I guess you answered one half of it, was TSA approach to cost.

But the other costs that have just been talked about here intrigued me, as to whether or not that cost will be sole-sourced to an existing contractor or will it be put on the market competitively for Registered Traveler?

Mr. HAWLEY. If we are talking about the April 20th deadline of finding the provider who will certify all of the proposals that come in, it is our intention to have that be open bid.

Mr. THOMPSON. So people who are doing that now have an opportunity to bid, just like anyone else?

Mr. HAWLEY. I believe so. It is subject to whatever the acquisition rules are and all that. But it will be a transparent process. And it is obviously a critical part of the security of the program, so it will be well-examined.

Mr. THOMPSON. So you do not anticipate sole-source contracting for the clearinghouse process?

Mr. HAWLEY. Well, for the clearinghouse process, there is, as you know, a requirement to use a particular clearinghouse. And from our point of view, we are agnostic on it, because it is a utility that does some work that we do not have to do and we do not pay for.

So the way it works—

Mr. THOMPSON. Who pays for it?

Mr. HAWLEY. It would be somebody down the line, either the provider who wants to offer the card or, potentially, it would be passed through to the consumer.

Mr. THOMPSON. That is my point. I guess, since we have authorized a particular contractor, do you have an opinion as to whether or not that is the best business model for TSA or anybody to use?

Mr. HAWLEY. We are not planning to provide money to it. So it really goes to Mr. DeFazio's point earlier, that it is not us who are picking these contractors. And that is why we are doing the private-sector model.

Mr. THOMPSON. Well, I guess if we do not mind, we have got the same problem, in that, if you being directed to it, is your directing—does that give you the authority to say, "No, this is too high"?

Mr. HAWLEY. We worked with this particular provider on a lot of other issues. And it is a smooth, functioning system. And it is not excessively costly. And I believe that they are very tightly managed by their ownership, in terms of making the fees be not more than the cost.

Mr. THOMPSON. Explain to me, when they come to you with a cost, can you say, “No, this is too much; our example says it should be half what it is”?

Mr. HAWLEY. Should that be the case, absolutely, sir, yes. It has not been a problem to date, and we have done it with other programs. And we have had discussions as to how we both would be looking at it. And I believe that we are looking at it in the same way.

Mr. THOMPSON. Well, I guess we will probably get some additional questions to you around this subject.

Thank you.

Mr. ROGERS. The chair recognizes the gentleman from Washington for some additional questions.

Mr. DICKS. Yes, I just wanted to go back to the watch list. Is it true that you have to guess that you are going to secondary inspection because you are on the watch list? I mean, does anybody know—are they told you are on this watch list?

Mr. HAWLEY. If they are a no-fly, they are.

Mr. DICKS. If they are a no-fly?

Mr. HAWLEY. Right.

Mr. DICKS. So how would you be—why would you be—if you are a no-fly, it means, obviously, you have done some bad things out there?

Mr. HAWLEY. Correct.

Mr. DICKS. And so only those people are told?

Mr. HAWLEY. Yes. The selectee process works today, that the random component is put in with the on-purpose component, and it all prints out the same way.

And that is meant to provide some privacy for the passengers running through the checkpoint, so, if somebody sees them with a selectee card, it does not look like, “Oh, you must have done something bad.” It is part random and part not random.

Mr. DICKS. I am told that you do not get off the list. You get a TSA letter saying you are not the person on the list. Then you have to present the letter to the airport personnel, who may not know what to do with your situation. Is that still the situation?

I mean, isn’t there a way to get the person off of the list, off of the computer list?

Mr. HAWLEY. If it is the selectee list, I would be—if a person is carrying a letter saying you are not supposed to be on a list, then that sounds like a problem. So I would be very interested to see your example or see if we can straighten out what it is.

Mr. DICKS. Yes, I am just curious, because we have had stories come to the committee, anecdotal stories, that this is what happens. And it is very hard to get in a situation where you are no longer called into question.

Mr. HAWLEY. Yes. There has been a change that we have done at TSA, in terms of our participation in the watch. And our participation in the watch list, the standard is, do we believe this person could be a terrorist? As opposed to, do we believe this person could be, you know, something other than a terrorist who did something we do not like?

So we have ramped way back on that. And I believe we have zero today from TSA. Although we do participate with other agencies, as they have reason to put people on watch lists.

We do not do that ourselves, except in circumstances where we suspect there is a terrorist connection. And then we ask the appropriate agencies to investigate it.

And then we back out. And if they elect to put the person on, they do or they do not. And we do not get involved beyond that.

Mr. DICKS. Thank you, Mr. Chairman.

Mr. ROGERS. Thank you.

There being no further questions, I want to thank you again for your time. I know you are busy. And I appreciate you taking time to come here.

As the ranking member indicated, there are going to be some, I am certain, some additional questions. We have got several meetings going on, so some of our members could not be here. The record will be held open for 10 days, so I would ask that, if somebody does submit a question to you, that you reply in writing so we can get it included in the record.

And thank you for your time.

And we will now move to the second panel.

Mr. HAWLEY. Yes. Thank you, sir.

Mr. ROGERS. The chair now calls up the second panel for today's hearing.

It includes Mr. Charles Barclay, President of the American Association of Airport Executives; Mr. Lawrence Zmuda, he is a Partner in homeland security for the Unisys Corporation; Mr. Steven Brill, Founder and CEO of Verified Identity Pass, Inc.; and Mr. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center National Office.

And we also had a person who could not participate who asked that his statement be submitted for the record. And without objection, I would like to ask that his statement, the EDS U.S. Government Solutions, be submitted for the record because he could not participate in our panel today.

And without objection, that is submitted.

[The information follows:]

FOR THE RECORD

SUBMITTED BY THE HONORABLE MIKE ROGERS

EDS U.S. GOVERNMENT SOLUTIONS

The Department of Homeland Security (DHS), Transportation Security Administration (TSA) has concluded five pilots for the Registered Traveler (RT) program. The purpose of the RT pilots was to test the use of fingerprint and iris biometric technologies for identity verification, efficient screening, expedited travel, and enhanced security for travelers. The pilots operated at five major airports in Boston, Washington, D.C., Minneapolis, Houston, and Los Angeles during the period from July 7, 2004 to September 30, 2005. The pilots were intended to last only 90 days, but were extended to provide for a more thorough assessment of the projected improvements in security and enhanced customer service for Registered Travelers. Participation of travelers was voluntary, and each was required to meet eligibility criteria and to submit personal information TSA.

EDS' ROLE

EDS implemented two of the TSA pilots at Boston's Logan International Airport and Washington, D.C.'s Ronald Reagan Washington National Airport, working in conjunction with American Airlines. EDS' successful pilot projects proved that the EDS solution, in fact, expedites the airport screening process for participating travelers and protects the privacy of their personal information. Based on EDS' 13 of piloting the solution at two locations, we have concluded the following key findings:

- Fingerprint and iris biometrics are effective in confirming the traveler's identity quickly, accurately, and with minimal inconvenience.
- Travelers, as indicated through their overwhelmingly positive feedback, appreciate the convenience of an expedited airport security experience.
- Travelers are willing to voluntarily give up personal information and their biometrics in order to receive expedited service.
- A sound process for enrolling and adjudicating potential Registered Travelers has been tested and proven effective.
- A sound process for integrating a Registered Traveler lane unto the TSA screening checkpoint has been tested and proven effective.

EDS has additional experience on other programs that support the above findings, notably at Ben Gurion Airport in Tel Aviv, Israel, and with the DHS' nationwide U.S. Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS). The sum total of our lessons learned argue in favor of a nationwide Registered Traveler Program that is well-founded programmatically and technologically. Such a program provides a real benefit to all airport security stakeholders—travelers, airports, airlines, TSA, and traditional airport screening personnel.

EDS' testimony to the Committee is respectfully submitted to provide advice and lessons learned as the government determines the future direction for Registered Traveler. We offer below our key observations and recommendations in the areas of program design, program processes, technologies, and additional considerations.

PROGRAM DESIGN

The following discussion of some key program design issues relates to how the government can best structure, administer, and fund the program on a nationwide basis.

Program Administration. A nationwide Registered Traveler program is a government program that involves the support of private industry in coordination with local airports. As such, due to security concerns and the traveler's view of the program, EDS recommends that DHS retain oversight, make policy decisions, and administer the program. This role is consistent with guidance provided by DHS in its Privacy Impact Assessment (PIA) of June 20, 2005. The PIA states, regarding the pilot (and as amended includes the private sector subpilot) that, "TSA's role will focus on conducting the initial threat assessment and periodic reassessments, as well as providing standards, threat assessment screening, and oversight." EDS is in agreement with this approach, especially with regard to threat assessments, and recommends the government continue in this role with the nationwide RT program.

Some administration challenges DHS may face include: providing help desk services to assist in resolving travelers' issues' resolving disputes that might occur between providers, airports, and travelers; and privacy concerns. Within the PIA mentioned above,DHS notes that, "after review of the experience with this and other RT pilots and prior to implementation of the final program, TSA will issue a new PIA informing the public of changes to the program resulting in an impact to personal privacy."

Funding Mechanism. Multiple options exist (as noted below) for funding a nationwide RT program, with one preferred, based on the pilot results:

- *Government funded and administered*—This structure replicates the structure of the Original five government-run pilots. DHS secured funding for the pilots and provided full administrative support to the program, including running the procurement and selecting the technology providers. This structure is costly to the government, but provides the greatest degree of program control and flexibility.
- *Fee-based, airport-administered*——This model has been used in the Private Sector Known Traveler subpilot at Orlando International airport, which began in June, 2005. DHS participated in the Memorandum of Understanding (MOU) process and the security assessment process; however, the airport maintained total administrative control over the procurement, implementation, and pilot operations. This model is less costly to the government than a government-administered program, but also limits control. While the airport profits under this scenario from a direct revenue stream paid by the technology provider, the lack of controls on consumer fees puts the traveler at a disadvantage. In effect, the technology provider holds a monopoly on that airport, is free from pricecaps, and is unregulated as to methods used to attract travelers. This model requires

safeguards for protecting consumer interests and holding providers accountable for meeting objectives. Significant efforts would also be required of DHS to provide oversight, enable interoperability, select the right technology partners, assist in planning the rollout, work with airports joining the nationwide network, and define stakeholders roles and responsibilities.

- *Fee-based, government-administered*—This structure has not been piloted or even widely discussed. It functions similar to the fee-based, airport administered model above, but instead provides DHS ultimate control and flexibility. DHS would collect and control fees paid by travelers; approve marketing tactics; and be able to run mini-pilots to adapt to policy changes and new mandates.

Based on knowledge gained during the pilots, a fee-based, government-administered model represents the best alternative for DHS' nationwide program. It allows DHS to operate the program based on cost recovery while the government maintains overall administrative functions and program control.

Policy Decisions. By vetting travelers through a security assessment in the pilots and deeming them "low risk," TSA allowed travelers to bypass random secondary screening. While beneficial, other screening procedures pose greater inconveniences, such as having to remove shoes and overcoats and taking laptops out of cases. A policy change could exempt RTs from such activities. EDS recommends DHS explore such policy issues.

PROGAM PROCESSES

The following discussion of key program process issues relates to how the program can best operate to the benefit of all stakeholders.

Enrollment. As the program rolls out to multiple sites, use of consistent enrollment procedures becomes critical. In particular, EDS recommends the development of standard procedures for: collection of biometric and demographic information; authentication of travel documents; designation of traveler eligibility; and responding to government security alerts. Standardization of tokens such as smart cards, so that they are easily recognized, aids TSA checkpoint screeners. Fees charged to travelers, if required, should be consistent across all airports and collected at enrollment.

Checkpoint Similarly, standard processes at all participating airports' checkpoints should be defined and mandated. Examples include processes for: how the screener, if present at the kiosk, is to greet the traveler; how the traveler uses the message prompts at the kiosk; how the traveler is assimilated back into the TSA checkpoint after completing verification; what travelers do if their verification fails; and how RT lanes are to be set up relative to the traditional screener lanes. Lack of uniformity in these areas ultimately detracts from the value of RT, which is to smooth the traveler's passage.

Interoperability. Travelers participating in the pilot were only able to use the system at one airport, their "home" airport, which posed no interoperability issues. EDS recommends that airports electing to use an RT system within a nationwide program receive interoperability specifications endorsed by DHS. Such specifications should define the technical requirements that enable an enrolled traveler to use systems nationwide, and exclude providers from using proprietary technology for local RT systems. EDS recommends the use of established U.S. and International standards for biometrics and smart cards. Further, EDS recommends that a compliance-testing certification be issued prior to implementation to make sure that systems satisfy all interoperability specification.

Program Linkage. In some measure, RT is in a position to benefit from emerging government specifications such as the Federal Information Processing Standards (FIPS) 201, which target government employees and contractors. EDS recommends that DHS assess various credentialing systems, such as employees and contractors. EDS recommends that DHS assess various credentialing systems, such as US-VISIT, Transportation Worker Identification Credential (TWIC), International RT, and others, to determine the feasibility of using a single credential across the various DHS initiatives. In addition, it is likely that their existing processes and standards can be of benefit to RT, even if those agencies are using different physical credentials.

Use of RT Data. The information provided by travelers is valuable and there exist many "potential" uses of data collected and stored in the RT system. EDS recommends that use of such data be carefully defined and that strong privacy measures be put in place. How traveler information will be used and how personal privacies will be protected must be made very clear. Important issues to explore:

how the RT data should be linked to criminal low enforcement data; how traveler movements are to be tracked; and how data can be used to effectively interface with rental car and hotel chains.

TECHNOLOGY

The following discussion of key technology issues relates to how technology can best be used within a nationwide Registered Traveler program. While the RT pilots proved that fingerprint and iris biometrics can quickly, accurately, and with minimal inconvenience, confirm the identity of the airport traveler, some technical issues must be surmounted when implementing a nationwide program.

Standards Compliance. Interoperability standards are essential for a nationwide program, and various U.S. and international standards are now under development. Examples of existing and emerging standards include the following: TWIC, Personal Identity Verification (PIV), and Machine Readable Travel Documents (MRTD). Importantly, significant differences exist between international (International Organization for Standardization [ISO]) and u.s. (American National Standards Institute [ANSI]) standards. EDS highly recommends that DHS evaluate these efforts as it defines appropriate standards for a nationwide RT program. While one given standard my not precisely fit DHS' requirements, EDS expects that portions of the above standards, such as those applying to biometric data, will be advantageous to DHS. Token-based. EDS implemented two different solutions during the pilots—at Logan Airport EDS tested a token (smart card) solution; at Reagan Airport EDS tested a token-less solution. In the token-less solution, the traveler presents a biometric sample, either a fingerprint or iris scan. The pilot solution searched the entire Reagan Airport database population of 2,000 enrollees for a match. While the token less solution accuracy rated only a few percentage points below the token solution, we anticipate more dramatic divergences in the large populations of a nationwide program and therefore recommend a token-based solution

Network Connectivity. The pilots were conducted using standalone systems without network connectivity. It was therefore a manpower-intensive effort to propagate security assessment information and traveler status information to each kiosk without a network. The standalone configuration would lead to unnecessary costs burdening the traveler. EDS recommends that a second phase of testing be conducted to assess how best to create nationwide network connectivity for a truly interoperable and networked system.

ADDITIONAL OBSERVATIONS

EDS delivered to DHS operational summary reports for the Boston Logan and Washington Reagan pilots on February 7, 2005. The reports contain nearly six months of performance measurements and observational data, which is valuable to consider as the program moves forward. For example, metrics are provided on the accuracy of different types of biometrics, and on the comparative duration of traveler crossings using card reading or biometric-comparison approaches. EDS also documented many implementation and operational lessons learned. These lessons closely match EDS' experience in providing registered traveler solutions for clients such as Ben Gurion Airport. EDS recommends that the summary reports be used to support decision-making. The following are examples of pilot lessons learned:

Stakeholder Management. The pilots involved not just travelers, but multiple stakeholders, each with their own concerns. These included: TSA Headquarters, TSA local airport operations, American Airines Headquarters, American Airlines local airport operations, and the airport authorities, Massachusetts Port Authority in Boston Logan and Metropolitan Washington Airports Authority at Washington Reagan. At these and all other airports EDS services, the most important stakeholder is always the traveler. EDS considers it critical to clearly define roles and responsibilities for each stakeholder and to identify a single point of contact for the airport RT program. EDS recommends that effective stakeholder management methodologies be put in place at project start.

Traveler Communications. While the program was well received by travelers, they indicated a need for timely communication. Travelers need an easy way to keep themselves fully informed about issues affecting them, such as: information on contract extensions, holiday hours, and future program direction. Travelers that were well informed of the program's availability exhibit high customer satisfaction.

Privacy. EDS's experience shows that airport travelers are highly interested in using biometric readers, either a fingerprint, iris camera, or had scanner, to confirm identity. They are anxious to use such solutions to speed their travel. They variously report concerns on the system's capability to safeguard and protect their information. This is their biggest concern and requires a trustworthy solution.

Conclusion

EDS has been proud to support the TSA in the successful pilots at Boston Logan and Washington Reagan Airports, and believes that their outcomes provide significant value to DHS as the Registered Traveler program moves forward. Based on feedback we received from travelers, they are grateful to be participants in the pilot projects and are now anxious to enroll in the nationwide program when it becomes available. EDS is anxious to support them in this valuable program.

Now the chair calls up Mr. Charles Barclay, President of the American Association of Airport Executives, testifying on behalf of that association.

And we look forward to your statement.

STATEMENT OF CHARLES BARCLAY

Mr. BARCLAY. Thank you, Mr. Chairman and members of the committee. I would like to make just three points.

First, that a Registered Traveler program, in the opinion of airports, is essentially an element of a secure and convenient future transportation system.

Security needs to be the first consideration. And, as the 9/11 Commission report stated, for terrorists, travel documents are as important as weapons. Having an accurate, verifiable, voluntary form of identification, especially for the busiest travelers in our system, has great value for reliably recognizing those who do not pose a threat to the system.

If one travels for a living or something close to it, the time penalty our new security procedures impose is multiplied over and over again. Much more than just an occasional inconvenience, it is a real loss of productivity.

Of the 700 million in plane passengers each year, 40 percent of them are made up by 5.5 million people, or 8 percent, according to the Air Transportation Association, and 50 percent of that 700 million are made up by just 8 million frequent travelers.

We use background checks for airport and airline employees, for federal air marshals and local law enforcement officials who carry guns on airplanes, and other individuals that we trust will work to keep the system safe.

We can certainly use the same policy for passengers willing to pay for their own security checks and volunteer information on themselves, to trust simply that they do not pose a danger to the system and provide them expedited screening.

My second point is that almost 60 airports, led by an executive committee of Minneapolis, Phoenix, San Francisco, Denver, the Washington airports, Dallas, Boston, and Columbus have organized a Registered Traveler Interoperability Consortium, or RTIC, to move the program forward.

Significant effort has been expended by these airports due to the importance of an R.T. program to them and the need to agree on some minimum standards among airports that wish to have their individual R.T. programs interoperate.

The RTIC members are intent on developing an open standard cost base platform that protects customers' interests and the airports' investments. As local government agencies involved, the airports have the appropriate public-sector incentive to serve passengers' security and financial interests in the program.

RTIC policy is to work closely with TSA. And we eagerly await TSA's policy and operating rules for its essential role in Registered Traveler.

RTIC has also formed a service providers council of private companies involved in R.T., to make sure that the best possible technical and business advice is provided to the airport members.

RTIC airports have adopted a policy, again, one that is consistent with their public agency incentives to empower as many private vendor solutions to the R.T. program as possible and establish a level playing field for all those vendors.

Let me parenthetically add on the MOU issue that Mr. Rogers raised, that the listing of points in our testimony outlines the way the RTIC members think the program should run.

If you read very carefully several sections, you will see we were not saying that there is an MOU, but our proposal is there would be an MOU, so that TSA would do the vetting of all the passengers, not anyone else in the system.

My final point is that AAAE, RTIC, and the Transportation Security Clearinghouse are ready and eager to facilitate R.T. with existing partnerships and resources.

There already exists a highly efficient, trusted security network that connects all commercial service airports, airlines, and the federal government for the purpose of employee security background checks and verification.

The clearinghouse collects, checks, transmits, tracks and accounts for the biometric and demographic information on employees with access to secure areas of airports. And it had a remarkable record of reliability and efficiency.

The clearinghouse has processed over 1.8 million criminal history record checks since January 2002, making it the largest security clearinghouse outside the Department of Defense.

Before 2002 and creation of the clearinghouse, criminal history record checks for airport and airline employees took an average of 52 days, almost 2 months. Today, the clearinghouse averages 4 hours. And that represents a huge savings in personnel costs to our industry.

The clearinghouse has reduced the fee per record from $31 to $29, of which $22 goes to the FBI, making this fee less than a third of what other transportation interests are paying for the same criminal history record check.

The clearinghouse has a number of other best-of-class and first arrows in its quiver that are detailed in an article[1] and some other information that I would like to also ask be made part of the record.

Building upon this established security network is a commonsense approach for quickly and efficiently enabling interoperable R.T. for airports. The clearinghouse is governed by RTIC policy and the airports that run that, requiring that it maintain an open, vendor-neutral standard.

[1] "Inside TSC: Saving Money Saving Time" Airport Magazine, May/June.

Airports and airport executives look forward to assisting the Congress and TSA in establishing a needed Registered Traveler program.

Thank you, Mr. Chairman.

Mr. ROGERS. Thank you, Mr. Barclay. And that will be submitted for the record, as well, along with your full statement.

[The statement of Mr. Barclay follows:]

PREPARED STATEMENT OF CHARLES BARCLAY

Thank you for the opportunity to share with the subcommittee the views of the airport community on the future of the Registered Traveler Program. I am testifying today on behalf of the American Association of Airport Executives (AAAE), Airports Council International—North America (ACI–NA), and our Airport Legislative Alliance, a joint legislative advocacy organization. AAAE represents the men and women who manage primary, commercial service, reliever, and general aviation airports. ACI–NA represents local, regional and state governing bodies that own and operate commercial airports in the United States and Canada.

I want to begin by expressing our appreciation to you, Chairman Lungren, and to the subcommittee for the considerable attention you have devoted this year to highlighting the need for the federal government to expedite the deployment of new technology, including the Registered Traveler Program, in order to improve the effectiveness and efficiency of security screening operations at airports across the country. With aviation traffic returning to record levels and with federal resources become ever more scarce, it is imperative to get the most out of the resources we devote to security. Utilizing better technology to effectively manage risk results in better security and a more efficient use of federal and industry investments.

Unfortunately, the federal government to this point has been slow to embrace the promise of technology as the subcommittee has heard during the course of several hearings this year. The in-line installation of explosive detection equipment in airports, for example, will save the federal government billions of dollars at the handful of airports where TSA has committed resources to having those systems in place. Despite significant security benefits and dramatic personnel savings—savings that could be applied to other homeland security needs—no plans yet exist for federal investment in these systems at additional airports.

The Registered Traveler Program has likewise been slow in gaining firm direction from TSA. We are, however, very encouraged by the leadership that DHS Assistant Secretary Kip Hawley has shown in this area and believe that we are finally moving in the right direction with this critical program.

Rather than waiting for government to act entirely on its own, it is clear that airports and the aviation industry can and should play an active role in partnering with the federal government to design and implement meaningful solutions to security challenges. The establishment of effective public/private partnerships has already proven extremely successful, for example, in building a system for processing fingerprint-based background checks and additional background screening for more than 1.8 million airport and airline employees through the Transportation Security Clearinghouse.

On the Registered Traveler front as I will discuss in more detail, the airport community and its aviation partners are moving forward to help provide a model for Registered Traveler programs that will be interoperable, innovative, and will endure past the span of a "pilot program." Undoubtedly, the best path forward is one in which federal resources and standards are combined with the knowledge, expertise and creativity of airports, airlines, and aviation-oriented businesses.

Registered Traveler Program Will Improve Security and Efficiency at Airports

The value of a nationwide Registered Traveler Program is already well-established. The concept has received the strong endorsement of the 9/11 Commission and numerous others as the subcommittee discovered through the various hearings you have held on the topic this year. In an era of risk management, limited federal resources must be focused on known and unknown risks to the aviation system. Registered Traveler accomplishes that goal by helping TSA to better align screeners and resources with potential risks.

In simple terms, Registered Traveler shifts the focus from finding dangerous "things" to finding dangerous "people." The most important weapon that the 19 terrorists had on September 11 wasn't box cutters; it was knowledge—knowledge of our aviation system and existing security protocols, which they used to their advantage.

With more than 700 million passengers traveling through the U.S. aviation system each year—a number that is expected to grow to more than one billion annually within the next decade—we simply cannot afford to treat each passenger the same. Today's personnel-dependent screening system is already being pushed to the brink, a fact that is evidenced by increased wait times at a growing number of passenger and baggage screening checkpoints. One can only imagine how bad the situation will become as 300 million or more additional passengers are added to the system—especially if they are processed as they are today.

While a nationwide Registered Traveler Program will be open to all whom are eligible, there is no doubt that the frequent fliers—the six million passengers who make up the overwhelming majority of all travel—will be the ones most likely to enroll. By providing a different screening protocol for this group of registered and scrutinized travelers—which we believe is a critical component of the program moving forward—TSA will be able to better target security resources, expedite processing for all passengers, and reduce the passenger "hassle factor."

As you know, TSA has just concluded a Registered Traveler pilot program that involved five airports partnering with a single air carrier at each airport. A sixth pilot program which involves a public-private partnership is on-going at Orlando International Airport. Although the original TSA Registered Traveler pilot programs were popular with participants, they were not interoperable by design, which severely limited benefits to only one air carrier at each of the five original airports. Additionally, participants were subjected to the exact same security protocol—the removal of laptops, shoes, and coats were still required, for example—as non-participants, meaning that the only real benefit was simply being moved to a shorter screening line.

Now that the technology has been tested, we should turn to a process that realizes the true potential of Registered Traveler, one that is ***nationwide and interoperable.*** Participants who sign up in Dallas, in other words, must be recognized and accepted as they travel to San Francisco, Los Angeles or other airports throughout the aviation system. Additionally, security screening protocols should be adjusted for program participants in recognition of the extensive background vetting they have received.

Airport Registered Traveler Interoperability Consortium (RTIC)

Airports, in light of their public nature and responsibilities to the communities they serve, remain eager to partner with the TSA to improve the effectiveness and efficiency of the security screening process. In recognition of the promise that Registered Traveler holds in achieving these goals, airport professionals have been working diligently to move forward operationally with the program. One voluntary initiative in particular that I would like to report to the subcommittee today is the creation of the Registered Traveler Interoperability Consortium (RTIC). The RTIC is a group of nearly 60 airports that are working to define and establish the mutual and common business practices and technical standards that will complement federal standards and help push forward a national program. This represents a significant attempt by a large group in the airport community to partner with TSA in making the promise of RT a reality as quickly as possible.

The goal of the RTIC is to develop a common set of business processes and technical rules on an open, secure and industry-driven network among airports that will create a fair and seamless platform for airports, airlines and vendors to interface with DHS and among each other. Rather than pre-ordaining any one proprietary system, this open-architecture approach ensures that airports have an opportunity to work with any number of technologies or vendors to design a system that works best at their facility. This approach also ensures that the creativity and competition of the private sector is unleashed to better serve local needs and to keep program costs in check.

Current members of the RTIC include:

Albany International Airport
Atlantic City International Airport
Bangor International Airport
Boston Logan International Airport
Chattanooga Metropolitan Airport Authority
Dallas/Fort Worth International Airport
Denver International Airport
Northwestern Regional Airport Commission
Palm Beach International Airport
Palm Springs International Airport
Peninsula Airport Commission
Philadelphia International Airport
Phoenix Sky Harbor Airport
Pittsburgh-Allegheny County Airport Authority

Dickinson Theodore Roosevelt Regional Airport
Flagstaff Pulliam Airport
Fort Wayne International Airport
Ft. Lauderdale-Hollywood International Airport
Grand Forks Regional Airport Authority
Greater Orlando Aviation Authority
Greater Rockford Airport Authority
Huntsville International Airport
Jackson Hole Airport
Kent County Department of Aeronautics
Lafayette Regional Airport
Lexington Blue Grass Airport
Lihue Airport
Las Vegas McCarran International Airport
Memphis-Shelby County Airport Authority
Metropolitan Knoxville Airport Authority
Metropolitan Nashville Airport Authority
Mid-Ohio Valley Regional Airport
Minneapolis-St. Paul International Airport
Monterey Peninsula Airport
Myrtle Beach International Airport
Northwest Arkansas Regional Airport
Port Authority of New York and New Jersey
Port Columbus International Airport
Pullman-Moscow Regional Airport
Redding Municipal Airport
Redmond Airport
Reno-Tahoe Airport Authority
Rhode Island Airport Corporation
Roanoke Regional Airport Commission
San Francisco International Airport
Santa Barbara Airport
Seattle-Tacoma International Airport
St. Louis-Lambert International Airport
Shenandoah Valley Regional Airport
Metropolitan Washington Airports Authority
(Reagan National and Dulles Airports)
Tucson Airport Authority
Tupelo Regional Airport
Waco Regional Airport
Wayne County Airport Authority
Wichita Airport Authority
Wilmington International Airport
Yeager Airport

The airports of the RTIC have established and agreed on common core principles that will enable technical interoperability across a broad and varied airport network. More importantly, these principles will establish processes and procedures that will provide a consistent, common and secure framework from which Registered Traveler can work for all travelers at airports choosing to participate in the RTIC. Specifically, the RTIC has agreed to create a system where:

- Qualified applicants in the RT Program will agree to voluntarily provide TSA—specified personal data, both biographic and biometric, which will be used by TSA to assess the security threat of each participant.
- Service providers will be responsible for enrollment operations, including collection and verification of personal data of eligible applicants. Service providers must protect and maintain all personal data related to an applicant in a secure manner and prevent the unauthorized disclosure of the personal data.
- Service providers must securely transmit valid application enrollment data to the RTIC Registered Traveler Management System (RTMS). The RTIC RTMS will receive enrollment data from the RT service providers and will validate and perform duplicate checking of received enrollment data and forward data to the TSA for security threat assessments.
- The TSA will conduct the security threat assessments and return results daily per a Memorandum of Understanding (MOU) between TSA and RTIC.
- On receipt of notification of an acceptable security threat assessment for an applicant, the RTIC will notify the RT service provider for that applicant of the updated status of the applicant and will forward the applicant's credential information to the service provider.
- Service providers will issue and deliver participants' membership cards (e.g. smart cards). Service providers must notify RTIC of any future changes in the status of their participants, such as lost or stolen cards. Service providers are also responsible for customer service, including communicating with applicants regarding their approval status and responding to applicant and participant inquiries.
- Service providers may not unnecessarily disclose biographic and/or biometric data required for the purpose of the RT Program and collected by the service provider from RT Program applicants or participants. Service providers may not sell or disseminate any biographic and/or biometric data required for the RT Program and collected by the service provider from RT Program applicants or participants for any commercial purposes without the approval of the airport.
- Participating traveler processing will occur at the airport's security checkpoints. The placement of the RT screening stations will be located in front of the TSA passenger screening areas. Passengers that are not enrolled in the RT Program or are not approved when presented at the RT processing area will use

the normal TSA security lines/lanes. Passengers that are enrolled and approved will use the designated RT security screening lines/lanes.

- Biometric technology will be used for traveler identity verification at the RT screening stations. Once a participant presents their membership card, fingerprint and iris biometric features will be used to verify passenger identity. Proposed biometric systems shall be currently operational, highly accurate, cost effective, and capable of confirming the identities of large populations within short time constraints.
- Service providers will operate the RT screening stations, including the timely update of system and card revocation status to ensure fast, secure and reliable verification and status-checking at the airport checkpoint.
- Service providers are responsible for installing, furnishing, integrating, operating and maintaining all of their required equipment and systems.
- The RTIC will create and maintain the technical and business rules for the RT Program. The RTIC will operate a certification program for RT service providers to validate the conformance of their systems, service levels, and processes with the RT Program rules. Service providers will be required to undergo an annual re-certification and auditing of their systems and processes.
- Service providers will market the RT program to potential applicants and will use standardized RT Program logos and signage within their marketing.

Other airports may choose other approaches. However, by establishing a sustainable and cost-driven approach in partnership with TSA, airports can help ensure a Registered Traveler Program that focuses on enhanced security above all else in addition to expediting the travel experience. These two pillars are the primary values that the nation's frequent air travelers want and that each of you as policymakers rightly will demand. By bringing efficiency back into the nation's airport screening checkpoints, TSA screeners will be able to better focus their limited resources on the critical task of providing more rigorous screening to individuals about whom we know less than those who have voluntarily submitted their background for extensive vetting and clearance.

As each member of this subcommittee knows as a frequent traveler, every airport is unique. A successful, long-term Registered Traveler Program depends on the implementation of a technical, operational and business model capable of supporting individual airport needs, while providing the common infrastructure that allows passengers to use this capability at any airport nationwide. In recognition of that fact, it is critical that a permanent Registered Traveler Program be airport-driven and run outside of government with careful and consistent government standards and oversight.

Mr. Chairman, more than four years after the tragic events of September 11, we still have a great deal of work to accomplish in transforming the existing personnel-dependent screening system into the system of the future. In an era dramatically increasing demands on our nation's air transportation system, it is critical that we move forward as quickly as possible with promising technology like the Registered Traveler Program. Airports and the aviation industry have a key role to play in working with the federal government to make RT operational, and we are pleased to report great progress in that regard. It is our sincere hope and expectation that the federal government will fulfill its responsibilities so that the program can become a reality in the very near future.

Again, we appreciate the leadership of this subcommittee and the opportunity to testify today.

For the Record

TRANSPORTATION SECURITY CLEARINGHOUSE

Industry-driven federal partnership
dramatically increases security and saves industry hundreds of millions of dollars

AAAE has recognized a new milestone in their successful security partnership with DHS. The Transportation Security Clearinghouse (TSC), a unique public-private partnership charged with strengthening the security and efficiency of aviation employee background checks, surpassed 1.8 million fingerprint-based background checks successfully completed. Since its creation in December 2001, ***the TSC has processed 1.8 million criminal history record checks for airport and airline***

employees and has saved the airport and airline industry both time and money through its commitment to efficiency and technological innovation.

In fact:

- The TSC process has reduced the time it takes for airports to get fingerprint results from an average of 52 days, pre-September 11 when submitting to OPM, to an average of 4 hours, with most reports completed in around 40 minutes. This reduction in time has enabled airports to put their employees on the job where they are needed, without the need to pull another valuable employee from their duties to serve as an escort. The TSC has ***saved the industry hundreds of millions of dollars in productivity gains*** and employee retention as a result of reduced fingerprint check processing times.
- Because of innovative in-house technical work, the TSC performs "real-time" processing to transmit fingerprints to the federal system in an average of 16 minutes. ***The TSC's "real-time" processing dramatically increased the efficiency*** and timeliness of the airport fingerprint submission process.
- Centralization of the fingerprint tracking process allows for accurate fingerprint submission status at any point in the background check process ***virtually eliminating "lost fingerprints" within the federal system.*** Ensuring that airport employees can return to work and not have to be called back for repeated fingerprinting due to missing fingerprints this centralized process has saved airports thousands of wasted employee work hours over the last three years.
- ***The TSC is paid by and works for the airports and airlines conducting employee checks, not by TSA.*** This affords the TSC the opportunity to make quick changes on behalf of airports without having to worry about going through burdensome TSA approvals for every change it makes to its process.
- TSC provided an ***industry first Virtual Private Network (VPN) connectivity for fingerprint submissions.*** This innovative approach which was provided by the TSC to airports free of charge connects the livescan devices at the airports to the TSC and currently saves some airports over $1,000 a month in long distance telephone charges.
- Because of AAAE's ability to do the technical and administration work "in-house" and subsidize labor and other costs for the formation of the clearinghouse, the resulting cost savings allowed TSA to ***lower fingerprint processing prices*** from $31 to $29 (for electronic submissions), ***saving the industry over $3 million dollars.*** The TSC has been working with TSA to reduce the processing fee to an even lower rate.
- FBI indicates that the submissions of the aviation community done through ***the TSC had one of the best error rates in the U.S. (2%)*** and that this reduced error rate was directly related to the quality checks and error corrections performed by the TSC. The current federal average error rate is 8%. Since the TSC began operations, the error rate has continued to decline, with a significant drop when the TSC brought its "in-house" developed software package online. This equates to approximately 32,000 aviation workers that did not have to go through the time consuming process of reprinting due to errors created at the airports' print office with a ***cost savings of $2.5 million dollars to the industry.*** The TSC also warehouses submitted fingerprints allowing correction and resubmission when errors occur between the TSA and FBI, saving industry valuable time, effort and more importantly saved labor costs.

The Transportation Security Clearinghouse (TSC) has been remarkably successful in providing one central location where the mandated task of checking the backgrounds of hundreds of thousands of airport and airline employees can begin. The TSC established a quick and secure method to collect employee fingerprints, user payment and offer customer service for over 500 airports and multiple airlines across the country for further processing by the FBI.

As demonstrated above, the Clearinghouse has taken a number of steps to make the process as easy and efficient as possible for the aviation industry. We facilitated the first high speed secure connection to the federal fingerprint processing system, set up and brought online over 500 separate submitting entities for fingerprint processing and have served over 1.8 million fingerprint records that were passed on to the federal government for processing at an average speed of 16 minutes per record.

The Clearinghouse is committed to continuous improvement and working with airports, airlines and government agencies on all the issues that impede a smooth-functioning criminal history record check process.

Mr. ROGERS. The chair now recognizes Mr. Steven Brill, Founder and Chief Executive Officer of Verified Identity Pass, for his statement.

Thank you very much for being here. We look forward to hearing what you have to say.

STATEMENT OF STEVEN BRILL

Mr. BRILL. Thank you, Mr. Chairman, members of the committee.

When we started our company more than 2 years ago to launch what we call the voluntary credentialing industry, we were hardly the ones thinking about Registered Traveler programs. Many on this committee and others in Washington were on the same path.

But our approach was different from most in one key respect: We agreed that the government should do the applicant threat assessment, but we did not believe that this should be a government program.

We did not believe that government could offer the efficiency, the customer service, the incentives for continual innovation, and the privacy protections that a robustly competitive private-sector industry could provide.

Last winter, the TSA authorized a private-sector program in Orlando. The airport went through a selection process and, in June, Verified Identity Pass, along with its partner and general contractor, Lockheed Martin, won that competition. And I emphasize it was competition.

Our service, called Clear, based its approach on price, $79.95—which was not computed in the way that the Congressman DeFazio has implied—intense customer service, a money-back guarantee, and, of course, the convenience of passengers.

We also concluded that Registered Traveler programs had to create brands that customers would trust, because this service involves both security and privacy.

Thus, among other things, we promised our members: First, not to track where and when they used the card; second, an identify theft warranty, covering our cost if their identities were compromised in any way by our program; and, third, not to do what I used to be able to do, and did, as a magazine publisher, sell or give their names to any other marketers.

Now, we backed these promises by appointing an outside, independent privacy auditor to issue public reports on how we are keeping those promises. We also appointed an ombudsman for our members to complain to. And, in fact, we offered the people from EPIC the job of being our ombudsman, because we wanted an open, transparent process.

We have now been operating the Clear program in Orlando for more than 3 months. We already have 10,000 enrollees and are well on track with our business projections for getting more than 50,000 members in the first year of the program.

According to an elaborate metric support that TSA required of us of covering the first weeks of the program, and as Administrator Hawley mentioned, the system and the technology works.

Equally important, our members have enjoyed a predictable, time-saving experience at the airport, and we have provided the committee with details of just how time-saving that experience is.

As you will see from copies of the feedback that we have received, the postcards, most of our members, it is no surprise, love the program. In fact, they really only have one major complaint, that it is not in more airports.

Now, it is good news that they love the program, not only for us, but for TSA and everyone who moves through an airport, even non–Registered Traveler members.

Here is why: First, as the Chairman stated in his opening remarks, because R.T. members are such frequent fliers, when R.T. reaches critical mass, it will eliminate a large, disproportionate amount of hay from the haystack that TSA faces everyday, as much as 40 percent of travelers on a given weekday morning, all in a program that costs TSA, the airports, and the airlines not a nickel.

Second, R.T. programs, when they are operated correctly, move all passengers through more quickly. The best analogy here is electronic toll-taking, because drivers who have an E–ZPass, as we call it in New York, move through the toll lanes faster. Their lanes can absorb more cars, which means that even those without E–ZPass now enjoy toll lines that are shorter.

The trick, of course, is to calibrate the right mix of E–ZPass and non–E–ZPass lanes so that the E–ZPass lanes do not get clogged as enrollment increases, and so it will be with R.T. at the airports.

Now, our lanes already do move faster, because Clear members are practiced customers and because we provide, at our expense, a concierge at those lanes to help them remove their cell phones and get their bins, et cetera.

But those lanes need to move faster for this program to work, and to achieve the full E–ZPass effect, and to give our customers the full benefits that they want and deserve, in return for agreeing to be vetted. These benefits include not making them remove their shoes, laptops, or suit jackets.

Fortunately, under Administrator Hawley, TSA seems to have expressed a willingness to make such changes, in keeping with the risk management that has been so much a part of Secretary Chertoff's articulation of DHS's urgent mission.

Now, we get to play our part, too, in speeding up the lanes. In addition to our concierge service, we plan, upon TSA approval, to finance cutting-edge, new technology that can speed people through our lanes at the same or better security level before TSA can then finance that same equipment at all the lanes.

Now, TSA already has done much to make a national Registered Traveler program happen. In the Orlando program, TSA developed specific but vendor-neutral technical standards that clearly present a blueprint for programs beyond Orlando.

And TSA, as you heard, has already declared that any programs going forward must be interoperable with others.

A month ago, I stood on the stage with our able competitor from Unisys, Mr. Zmuda, at the ACI convention in Toronto. And we both pledged that we would and could achieve that interoperability.

And we will, because it is in our interest to do so, just the way it was in the interest in banks to achieve interoperability for ATM machines.

Now, I will close by noting that interoperability is also a key to ensure the thing that I know everyone on the committee, and particularly Congressman DeFazio, is worried about, and that is robust competition.

If a competitor who operates a Registered Traveler program at O'Hare Airport knows that, because all cards are interoperable, he could also sell cards to people in Dallas, where there might be a Clear program at that airport, then that competitor could set up shop in downtown Dallas and compete with us at Clear.

So how do we go forward? Well, I can tell you that, if TSA mapped a clear blueprint for benefits to R.T. members and then allowed airports or airlines, where the airlines control their own terminals, to present programs to TSA for vetting and approval, we and our competitors would likely be rolled out at 30 or 40 of the 50 largest airports within 6 months, and just as many small airports, because there is an economic model we can use for small airports, as well.

In fact, we and Lockheed Martin have already begun assembling teams to do that kind of roll-out. This could soon mean 8 to 10 million people enrolled in Registered Traveler programs.

Now, that kind of critical mass would set the stage for this credential to be recognized at other venues, such as sports arenas or train terminals, that now cannot do much about security because they have no way to manage risk, other than searching everyone or searching no one.

So we hope that Congress will encourage and support TSA as it moves ahead. We hope that the legislative and executive branches will set tough standards, including making sure that competition is always encouraged and that any rules or mandated processes that inhibit competition, artificially raise costs, or threaten privacy are absolutely avoided.

That way, costs will stay low and critical mass, service level, and privacy protections will stay high. Then, with all respect, we hope you will stand back and let us compete.

Thank you.

[The statement of Mr. Brill follows:]

Prepared Statement of Steven Brill

Chairman Lungren, Congresswoman Sanchez, and members of the Subcommittee, I want to thank you for affording me this opportunity to sketch my vision of how a private sector voluntary credentialing industry can and should develop in the coming months across the United States and around the world—and to report on its first rollout, at the Orlando International Airport. My name is Steven Brill. I am the Founder and CEO of Verified Identity Pass, Inc., the company that created Clear, the first branded consumer product in the voluntary identity credentialing industry. It is also the company that launched and now operates the private sector Registered Traveler program at the Orlando International Airport, the first of its kind and now the only existing Registered Traveler program in the country.

A Different, Private Sector Approach

Of course, since we began our company more than two years ago, my colleagues and I have hardly been the only ones thinking about trusted or registered traveler programs at airports, under which people could volunteer to be pre-screened and get a biometrically secure card that would allow them expedited access through security. Many members of this committee and others in Washington were on the same path.

But from the beginning our approach has been different in several crucial respects:

Most fundamentally, we did not believe this should be a government program. Yes, the government should be responsible for the security vetting and threat assessments necessary for such a program. But for several reasons we believed then, and now, that this should not be a typical government program, wherein some contractor gets billions of dollars to create a new bureaucracy.

First, government shouldn't necessarily pay for such programs. Our program is based on the absolute principle that we are not seeking any government contracts or any government subsidies at all. We believe that these programs should not cost the taxpayers a nickel.

Second, it is hard to imagine that the government could offer the efficiency, customer service, incentives for continual innovation, and privacy protections—about which I will talk more in a minute—that a robustly-competitive private sector industry could provide.

Third, many of the security bottlenecks, if not now in the future, are in venues that the federal government doesn't and shouldn't regulate, such as sports arenas or office buildings.

Fourth, one government program would mean that one data base could track people's movements.

The Orlando Program:

Thus, even as TSA was beginning the funding of its pilot projects at five airports across the country—an initiative we applauded, because it tested the concept and the technology of Registered Traveler—we began urging TSA that the logical follow-on to these pilots was a private sector program.

Unlike the five pilots, this program would test the marketplace.

Would customers buy such a program?

Would they like it?

Could the marketing be appealing in a way that did not exploit fears or the current necessity of bottlenecks?

Could privacy and security protections be put in place?

Would the system actually work?

Could the technology—never before tested on this scale—work so that people could have their biometrics captured efficiently and accurately at enrollment?

Would the card-presentation process at the security lanes work?

Would the program cause wait times at non-RT lines to be longer?

Last winter, TSA agreed to consider such a program and approved Orlando as the site of its initial launch. The Greater Orlando Aviation Authority then went through a competitive process to decide who the service provider would be. In June, Verified Identity Pass, along with its general contractor and equity partner, Lockheed Martin, won that competition against the contractors who had ably implemented the five pilot projects.

CLEAR's appeal to customers is based on price ($79.95 a year, which is at the low end of what our research said frequent flyers might pay), intense customer service, a money-back guarantee, and, of course, convenience. It was also based on creating a brand that customers would trust—something that we believed, and knew from extensive focus group research, was especially important because we were selling a service that had to do with both security and privacy.

Indeed, we approached the privacy issue aggressively, for two reasons. First, we believe in strong privacy protection. (I am a long-time, card-carrying member of the ACLU.). Second, in talking to prospective customers across the country, we knew that it mattered to them, a lot. Thus, among other things, we promised our CLEAR members—by contract in their membership enrollment—

Not to track where and when they use the card;

An identity theft warranty covering any costs they might incur if for some reason their identities were compromised by our program.

Not to do what I used to be able to do as a magazine publisher—sell or give their names to other marketers.

And we backed the promises by appointing an outside Independent Privacy and Security Auditor to issue public reports on how we are keeping these promises.

Orlando Results So Far:

We have now been operating CLEAR in Orlando for about three months. And we already have more than 10,000 enrollees. We are well on track with our business projections for getting more than 50,000 members in the first year of the program.

TSA has required the Orlando Airport to have us keep elaborate metrics of the first weeks of the program so that TSA can evaluate it. Here are some highlights:

It typically takes a CLEAR applicant about 15 minutes to complete the first phase of enrollment—which happens at home or in an office on their own computers, where they establish an account and provide basic personal identifying information.

It then takes them only another eight minutes at the Airport to complete in person enrollment at our enrollment stations—wherein they provide their identifying documents for verification, and then have their fingerprints and iris scans captured.

We would be glad to provide more details, but I can tell you that the number of technical glitches in capturing these biometrics or in authenticating people at the security lanes has been minimal to non-existent. And our members typically spent four seconds and never spend more than three minutes waiting to go through security, whereas non-members often spent more than thirty minutes.

Thus, our customers are, to put it mildly, highly satisfied. We know that because as part of our customer service program every member who goes through the CLEAR security kiosks is given a self-addressed feedback post card. As you will see from the handout you have been given of copies of every one of the hundreds of post cards we have received (though with the names blacked out to preserve privacy), most love the program. The major complaint they have is that it is not in more airports.

Every week I call several of them myself to get my own feedback, and I can report that if these people are any indication, there are millions of people across the United States ready to sign up with us or our competitors.

That isn't just good news for us. It's great news for TSA and for everyone else—including non-enrollees—who move through an airport.

Here's why:

First, our surveys of enrollees in Orlando indicate that they use just that airport 40 times a year. This means that they are super-frequent flyers. What that in turn means is that when we get to 40,000 or 50,000 enrollees—and we will, especially once they can use the card at more airports—they will represent twenty to forty percent of the people using the Airport on any given weekday morning. That means that we will have eliminated a large, disproportionate amount of hay from TSA's haystack—20–40% of the crowd that they will have to pay slightly less attention to so that they can concentrate on those whom they do not know.

With that in mind, let me mention how I think Registered Traveler fits with and complements a program like Secure Flight in a way that also helps TSA and the traveling public: If Secure Flight is established, anyone making a reservation who is a member of an RT program could provide his or her unique RT account number. The resulting boarding pass the person would get (online or at the airport) would have a highly visible "RT" on it, which would allow, and in fact require, that person use his card at the RT lanes at the Airport. At the same time, the person's reservation process would be exempt from the usual Secure Flight process, in which a threat assessment is presumably made each time the person books a flight. That's because a threat assessment has already been made by the RT program, an assessment that is continually updated by the RT process. So, the person would present his RT card and biometrics at the RT lane. This could mean that 20 or 30 or 40 percent of travelers, once RT grows, would not have to be in Secure Flight and, in fact, be going through a more secure process than Secure Flight, because the use of the biometric card always insures the proper identity.

And suffice it to say that until a program like Secure Flight is implemented, RT is the only process by which we can provide threat assessments that are more efficient than the current system. So either way—before Secure Flight or once Secure Flight happens—RT represents a significant enhancement of TSA's risk management efforts.

Second, RT programs, when they are operated correctly, can actually help move ALL passengers through the airport more quickly. The best analogy here is electronic toll collecting, or E-ZPASS as we call it in the New York area. Because E-ZPASS drivers move through the toll lanes faster than others, their lanes can absorb more cars—which means that the non-E-ZPASS drivers now typically contend with toll lines that are shorter than before E-ZPASS. Put simply, because of E-ZPASS everyone goes over the Triborough Bridge faster.

The trick here is to have the right proportion of lanes between E-ZPASS and non-EZPASS and when volumes dictate shift lanes. And so it will be with RT at the airports. So far, we have been the beneficiary of extraordinary on the ground cooperation with TSA leaders and staff in Orlando, who are constantly working with our CLEAR staff to give us a dedicated lane when we need it and share it when we don't. And we are employing elaborate traffic flow models so that we can tell TSA what those needs are likely to be at each checkpoint at any given time of day when we have 15,000 CLEAR members or 30,000, or 50,000.

So, that's the simple answer to the oft-asked question of what happens to RT members when the program gets so popular that their lanes get clogged: as with E-ZPASS you anticipate that and change the lane mix.

During busy hours our lanes now do move faster because CLEAR members are practiced customers who "know the drill" of going through security—and because we provide our own concierge at the lanes during busy hours to help them with removing laptops and the like, and getting the bins they need to put their materials through the X-Ray.

Going Forward:

I mentioned to you that insofar as we have customer complaints it is typically that they want the program at other airports.

There's another complaint: They also want benefits that go beyond the significant one of having their own line and lane—and not being subject to second screening. Business travelers, who often make reservations at the last minute or change flights, are frequently subject to being selectees, and they do appreciate this benefit. But they want and deserve more.

And if they don't get it, we can't promise to move them faster through their lanes—thereby providing the benefit to non-members of having our lanes absorb a disproportionate share of traffic. Our concierges help speed things, but ultimately we need more.

Think of it as a bargain. Prospective RT members are willing to give up some of their time to enroll and some of their money, plus some of their personal information (albeit less than they give a credit card company) in return for moving through security lanes faster. In return, TSA ought to be willing to give it to them, because this allows TSA to remove much of the hay from the haystack.

Fortunately, TSA seems to get it. Under Administrator Hawley, TSA has expressed a willingness to provide more. TSA has said in recent weeks in various forums that they are considering amending the Standard Operating Procedure at RT lanes, for example, to allow for members not to have to remove shoes or laptops or take off their suit jackets. Another change under consideration is allowing RT members to go through security without boarding passes, so that they can meet passengers at the gate or accompany them there, attend conferences in airline lounges, shop in these areas, or use kiosks at the gate to obtain boarding passes. We know many airports, including Baltimore Washington International Airport and Pittsburgh International Airport, would welcome this option.

I should add that those changes in the operating procedure at the lane can only be possible where a program is successful enough to have enough critical mass to allow for dedicated RT lanes without making the other lanes and lines more congested. After all, changing the procedure at a lane will be hard if not impossible if the lane is not dedicated.

Which is why pricing, privacy policies and customer service are important not just for us as a business but for the success of the program as a whole.

It is also why imposing any extra fees from the government or entities designated by the government beyond their actual cost needs to be prevented. A program that costs too much and scares people on issues of privacy will not attract enough members to make these benefits possible.

So, I am hopeful, especially now that TSA has had more than a month to study the metrics report they requested to evaluate the Orlando program, that we will soon hear a comprehensive plan for TSA that addresses these issues by implementing the risk management that has been so much a part of Secretary Chertoff's articulation of the Department of Homeland Security's urgent mission. I'm confident that this will happen, first, because TSA set the stage and incubated this new industry with its pilot projects, and, second, because I know that the leaders at the helm, whom I observed first hand for more than a year while writing my book, are forward-looking and determined to deliver on this kind of common sense approach.

We are also eager to play our part in speeding up the lanes. I already mentioned our concierge. But on top of that we have expressed a willingness, indeed an eagerness, to finance cutting edge new technology at our lanes that could speed people through at the same or better security levels. For example, if a certain new technology allowed people to go through without taking jackets off because it could identify explosives as well as threatening metal objects, but if that equipment was too expensive for TSA to roll out at this stage, we might finance it. And I can report that we are in discussions with a variety of airport security technology leaders to propose exactly that kind of RT lane enhancement at various airports.

That's what the private sector and free markets do: give incentives to people like us to invest in ways that give continuing, added value to our customers—especially when, in our case, our customers have annual "subscriptions" that we have to get them to renew every year.

Beyond its sponsorship of the pilot projects, TSA has already done much to make a national Registered Traveler program happen. In the agreement it worked out with the Orlando Airport for a plan of operations it insisted on highly specific but vendor neutral technical standards that clearly present a blueprint for programs beyond Orlando.

And TSA has already declared that any programs going forward must be interoperable with any others. That means that if someone with a card sold by a competitor of ours who operates a TSA-sanctioned program in, say, Chicago, shows up at the Orlando airport, we have to work with that competitor to figure out a way to recognize that card. A month ago I stood on a stage at the Airports Council International meeting in Toronto with our competitor from Unisys, which bid against us in Orlando. We both pledged that we would and could achieve that interoperability. Which we will because, just as it was in the interest of banks to figure out ATM interoperability, it is in our interest to do so. We'll also achieve it because TSA is going to require it.

Other groups, such as the American Association of Airport Executives, Airports Council International, and a group that we and other service providers recently began to organize, called the Voluntary Credentialing Industry Coalition, or VCIC, are now engaged in nailing down these interoperability standards. As long as TSA makes us do it and helps us to do it by providing the technical standards and the framework for the rules of the road, this is not going to be difficult, especially with the aid and encouragement of groups like AAAE and ACI.

Interoperability is not only logical and doable but is also a lynchpin of what the most important feature of this new industry ought to be: competition. If a competitor who operates an RT program at O'Hare Airport knows that, because all cards will be interoperable, he could also sell cards to travelers in Dallas where there might be a CLEAR program, then that person could set up shop in downtown Dallas and compete with CLEAR. That means we will always have to be worried about what I consider to be the three competitive aspects of the service, in this order: Privacy Protection, Pricing, and Customer Service.

So how do we go forward? Well, I can tell you that if TSA mapped a clear blue print for benefits to RT members and then allowed airports or airlines (where airlines control their own terminals) to present proposed programs for approval, we and our competitors would likely be rolled out at 30 or 40 of the 50 largest airports within six months. We and our partner and general contractor, Lockheed Martin, have already begun assembling teams to do that in anticipation of a go-ahead from TSA. I assume our competitors have, too.

This could ultimately mean eight to ten million frequent flyers enrolled in RT programs. And it would set the stage, once this critical mass is achieved, for this kind of credential to be recognized at other venues that now cannot do much about security because they have no way to manage risk other than searching everyone or searching no one. For example if a large percentage of business people in a city were enrolled in such a program, it might be possible for a sports arena to recognize the cards because twenty to forty percent of its attendees might have one. So it could initiate a security program to address those who don't have one.

With that in mind, I know the prospect of business people not waiting on line for a basketball game while everyone else does presents images of elitism. But another way forward for these programs that we are working on is the ability to charge little or nothing to people who have already been screened by some governmental entity and provided their biometrics. Thus, perhaps law enforcement officers, or firemen, or hospital workers, or hazardous materials truck drivers could have that card at little or no extra cost because they are already screened.

So what should Congress do? Well, first, Congress need not appropriate a dime. We believe strongly that TSA should charge us fully for its costs to supervise these programs and vet all applicants.

But Congress should encourage and support TSA as it moves ahead.

Then Congress and the executive branch ought set strict standards and keep a watchful eye on competition. Any rules or processes that inhibit competition, artificially raise costs, or threaten privacy should be avoided, so that costs will stay low, and critical mass, privacy protections and service levels will stay high.

And then, with all respect, Congress and the executive branch should stand back and let us compete.

Thank you for allowing me to appear today.

Attachments—Verified Identity Pass, Inc.

Metrics Report

This report presents the highlights of the various metrics that the Transportation Security Administration (TSA) has asked the Greater Orlando Aviation Authority (GOAA) to have Verified Identity Pass collect during the first two months of the program.

The report is based on data collected between June 22 and September 16, 2005, and covered approximately 8,500 customers who completed an application for the program during that time. Enrollment began at the Orlando airport on June 22, 2005.

Customers began going through verification lanes on July 19, 2005.

What These Numbers Mean:

The typical Clear Member travels once a week from the Orlando airport. It typically takes them about fifteen minutes to enroll on-line and then eight more minutes to complete enrollment in person. They experience little or no trouble having their fingerprints and iris scans captured at the Clear Enrollment Center, or at the security checkpoints, where the clearance process of inserting their cards and being authenticated takes about 14 seconds from the time they are greeted there by Clear personnel. They are generally highly satisfied with the Clear product and process and Clear's customer service. And they are saving as much as twenty-nine minutes going through the security process at the Airport during the Airport's busiest times. Most important, they are assured of a consistently predictable experience going through security; their wait time has never exceeded four minutes and sixteen seconds and is typically just four seconds.

- Frequency of Air Travel: **3.8 trips per month**

When asked in an anonymous survey at enrollment how many times in the last month they had departed from the Orlando International Airport our members reported an average of 3.8 such trips in that prior month. This means they are highly frequent fliers. It also means that on any given day they will represent a high percentage of the travelers using the Airport. (Note: this metric was not gathered as part of the TSA request for data.)

- Average Time Spent Completing On-Line Enrollment: **14:56**

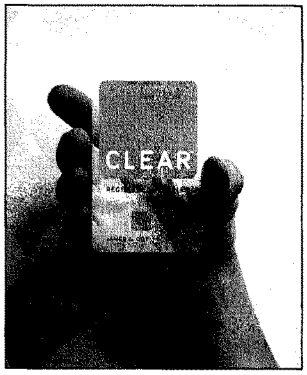
(Note: This is the time spent by an enrollee filling in basic person information on his or her computer before coming to the airport to complete in-person enrollment.)

- Average Time Spent For In-Person Enrollment: **8:31**

(Note: This is the time spent by an enrollee coming to the Airport and providing fingerprints, an iris scan, and his or her identification documents for authentication.)

- Average Success Rate for Capture of Fingerprints at In-Person Enrollment:

Attachments – Verified Identity Pass, Inc.



Greater than 99%

- Average Success Rate for Capturing Iris Image:

Greater than 99%

Demographics of Clear Members

- Gender

  - Male: 72.35% (4829)
  - Female: 27.65% (1846)

- Age

  - 0-20: 06%
  - 21-40: 23.12%
  - 41-60: 64.69%
  - 61-80: 11.52%

- Clear Members through the lane per day:

Max: 472
Average: 165

(Note: This number is rising rapidly as enrollments increase and new members receive their Clear Cards. For example, on Monday October 17, there were **580** trips through the Clear Lane.)

- Customer Satisfaction of 133 Respondents (Scale 1-10)

Line Wait: **9.6/10**
Ease of Use: **8.5/10**
Lane Layout: **8.8/10**
Enrollment Process: **7.7/10**

- Average Time To Authenticate Clear Card at Checkpoint: **14 seconds.**

- Time Spent Waiting To Go Through Security:

	RT wait time	Non-RT wait time
Maximum	**3:00**	**31:48**
Average	**:04**	**4:16**

Clear Members as of September 16, 2005: **8,500**
Clear Members as of November 1, 2005: **10,000**

Mr. ROGERS. Thank you, Mr. Brill.

The chair now recognizes the gentleman from homeland security at Unisys, Mr. Lawrence Zmuda, for his statement.

STATEMENT OF LAWRENCE ZMUDA

Mr. ZMUDA. Thank you, Chairman Lungren and distinguished members of the subcommittee. Thank you for the opportunity to testimony today.

My name is Larry Zmuda, and I am a partner at Unisys. I am proud to have led Unisys in its participation in the Registered Traveler pilot program sponsored by TSA.

In the spring of 2004, TSA competitively awarded to Unisys the contract for the Registered Traveler program. During the operation of those pilots, here is what we have found.

First, working with Northwest Airlines in Minneapolis, United Airlines in Los Angeles, and Continental Airlines in Houston, we saw first-hand how the airlines embraced this program.

Second, and perhaps more significantly, we were overwhelmed by the traveling public's support of programs to expedite the airport security checkpoint. Travelers voluntarily lined up and provided biographical information and biometric data, their fingerprints and iris scans.

The results of the program demonstrate three important benefits, including efficiency and convenience for air travelers. Wait times could be calculated in seconds rather than minutes. Enhanced security, TSA's screeners could focus their attention on unknown travelers, rather than travelers who had undergone background checks.

And third, effective technologies. The use of dual biometrics and smart cards produced the successful verification rate of greater than 99 percent.

Finally, the airport community has been equally enthusiastic. To date, more than 50 airports have pledged their support to the Registered Traveler Interoperability Consortium that Mr. Barclay and AAAE are spearheading. They see the benefits their customers are receiving and realize it is another way to improve their business.

While the benefits of the Registered Traveler program are apparent, successful expansion of this program through the entire country would require the participation of the private sector, especially in the area such as upfront capital assessment.

Successful implementation will require several millions of dollars worth of upfront capital investment at each airport. This includes the costs of developing, testing, marketing and deploying necessary technology and business operations.

Interoperability. One key feature for the traveling public is nationwide interoperability, being able to use a card in airports across the country. Just as one can use ATMs at competitors' banks, the same must be true in this case with airports.

By permitting multiple companies to participate, Registered Traveler will reap the benefits of competition. And the best solutions will be brought to the public. The private sector must help determine these standards and make them uniform and public so that all can benefit.

Subject matter expertise. The private sector has an abundance of subject matter experts who can assist in determining standards that will streamline today's capabilities and that also will examine and predict the program's future.

And finally, data privacy and assurance. We understand that privacy of personal data is critical. The private sector must not and cannot own the data of those enrolling in the program, but we must ensure that it is safe and secure while it is in our possession.

Certainly, the Congress and the TSA must retain their historic role in maintaining passenger security and privacy. I hope that TSA embraces this opportunity to leverage the private sector, for the benefit of the traveling public, our airports, the airlines, and TSA itself.

In a competitive environment, the private sector can facilitate the expansion of the Registered Traveler program, helping to bring the best solutions and utilize the most effective technology in the most cost-efficient manner.

Thank you again for the opportunity to testimony. Unisys looks forward to assisting the government agencies and lawmakers, as you continue your work in securing America's air travel.

[The statement of Mr. Zmuda follows:]

PREPARED STATEMENT OF LAWRENCE J. ZMUDA

The Role of the Private Sector in the Rollout of the Registered Traveler Program

Chairman Lungren and distinguished members of the subcommittee, thank you for the opportunity to testify today before this subcommittee about the role of the private sector in the Registered Traveler program. My name is Larry Zmuda and I am a partner at Unisys U.S. Federal Government Group. I am proud to have led Unisys in its participation in three of the five TSA-sponsored Registered Traveler pilots.

Unisys supports many of the initiatives that are critical to securing this nation in the post-Sept.11 era. We have worked on securing cargo entering the country, identifying non-visa immigrants as they leave the country in the US-VISIT program, and, via the Registered Traveler program, have helped frequent travelers gain an expedited and predictable experience as they proceed through the security checkpoint. Because of Unisys participation in these programs, we understand and appreciate the balance required to ensure secure travel within our borders without impeding commerce.

In the spring of 2004, TSA competitively awarded to Unisys the contract for the Registered Traveler program. Five days after award, we began enrolling travelers.

We worked with Northwest Airlines in Minneapolis/St. Paul, United Airlines in Los Angeles, and Continental Airlines in Houston. We saw first hand how the airlines embraced this program and, more importantly, how the traveling public willingly provided biographical information and biometric data—their fingerprints and an iris scan—to expedite their security checkpoint experience. During the operation of these pilots, Unisys was in a unique position to understand the technology and its impact on the various stakeholders: TSA, the airports, the airlines, and, most importantly, the traveling public.

We were overwhelmed by the number of travelers voluntarily lining up to register for this program. In Minneapolis, we enrolled almost 2,500 people in one week and had demand for more. For the pilots, though, TSA placed a cap on enrollments. All of the pilots, including the one in Orlando, have an enrollment limit. Notwithstanding this limit, the pilots that Unisys led provided some valuable metrics that validated this program. Enrollment and verification were quick and efficient. Travelers enrolled in less than 10 minutes and wait time at checkpoints could be calculated in seconds rather than minutes.

The pilots also showed how dual biometrics—in this case, fingerprints and iris scans—were critical in providing this service. Success rates were greater than 99 percent when dual biometrics were employed for identification. Additionally, the pilots tested smart card technology. Smart cards enhance security and capacity of the system. They?re also more cost-effective in a nationwide program.

The demand to continue and expand this program is unmistakable. Initial feedback from participants in these first pilot programs was consistent. "When are you going to expand this to other airports around the country?" was the common cry in e-mails and discussions we had with them. In addition to the traveling public, the airport community has been equally enthusiastic.

To date, more than 50 airports have pledged their support to the Registered Traveler Interoperability Consortium (RTIC) that Mr. Barclay and the AAAE are spearheading. The airports see the benefits their customers are receiving and realize it is another way to improve their business.

The benefits extend not only to the participating airports, but to the economy as well as the traveling public for faster security processing.

nce they've moved quickly through the security checkpoint, the travelers have more time to do work, shop at the stores, dine in the restaurants. This economic trickle-down effect is beneficial for local and national economies.

From a security perspective, improved process flow at the airports not only lessens the burden of the traveler, but of TSA. Because the registered travelers are known quantities, screeners can concentrate more attention on those travelers not known to them.

However, the airports and the TSA cannot perform all the requirements necessary to expand this program throughout the country. As with the five pilots, the private sector plays an important and critical role in the future of Registered Traveler to expand quickly and smartly across the nation.

Companies such as Unisys must be the driving force in the following areas:

- Capital investment
- Technology development
- Subject matter expertise
- Data privacy assurance

Financing for this program ultimately will come from those deriving the benefit, the traveling public. However, prior to taking a single fingerprint or iris scan and, therefore, one fee payment, significant capital investments must be made. All of the features of the program must be ready on day one. The solution must be built, tested and deployed. It is important to note that TSA always envisioned that Registered Traveler would be fully funded by fees and, therefore, not dependent upon Congress for funding.

The personnel who will enroll and aid the travelers at the checkpoints must be trained and paid. Work with communications and marketing firms regarding ways to reach the potential customers must begin. The business and operational processes must be in place to ensure smooth operations. All of these components combine to give people confidence that this is a program that will provide benefits without compromising security.

Several millions of investment dollars per airport are required to provide these capabilities. This is where the private sector can participate. Companies like Unisys understand all of the fiscal components and potential risks to smartly provide the capital investment required to launch this program. These are areas of expertise resident in the private sector; the government shouldn't be required to execute marketing or provide the latest biometric technologies. The federal government must devote its limited resources to providing security for all transportation modes.

Registered Traveler must allow multiple companies to participate. Competition will bring the best solutions and programs to the public. But competition must not bring with it solutions that do not work together. The technology that is developed and deployed at one airport must be interoperable with other Registered Traveler systems at other airports. This is the way to create a nationwide system.

The true benefit to the traveling public is interoperability—being able to use a card in airports across the country. Just as one can use ATMs at competitor's banks, the same must be true with airports. A registered traveler card issued by company X at airport Y *must* be able to work at another airport. The private sector must determine these standards and make them uniform—and public—so that all can benefit.

The private sector has an abundant supply of subject matter experts who can assist in determining standards that will streamline today's capabilities and that also will examine and predicts the future of the program. We must ensure that the technology is scalable and built in an open framework to handle the increasing volume should the program grow to the potential we are all anticipating.

This open architecture must be flexible enough to mesh with other federal programs and DHS initiatives, such as U.S.-VISIT, and potentially international programs looking to integrate with the United States. It would be untenable for programs not be interoperable after millions of dollars have been invested in them. Further, the technology must be accepting of new technology vendors as they enter the market. With many of the patents iris vendors hold about to expire,, this could be critical in enabling all providers capable of participating in the program.

The private sector also can be the test bed for the latest technology. The program presently utilizes fingerprints and iris scans as the biometric verifiers. Technology must constantly stay ahead of the game to ensure the program remains secure. Radio frequency identification—RFID—capability and facial recognition are just two technologies that are gaining acceptance and could play a major role in near-future verification. The expertise resident in the private sector would help minimize risks associated with deploying new technology in a program that revolves around security.

Finally, the public is very concerned about providing sensitive personal data. Supporting that concern are an untold number of database hacking instances over the past year. The private sector must not and cannot own the data of those enrolling in the program, but we must ensure that it is safe and secure while it is in our possession. Every component of the solution that can accept personal data such as credit card numbers and addresses must be thoroughly secure. As the data necessary to perform the background checks is transmitted to TSA, encryption must be employed to prevent outside parties from gaining access to and tampering with the data. No one—neither the government nor the private sector—wants to be part of the public outcry that would ensue from such a situation.

My hope is that TSA embraces this opportunity to work with the private sector. TSA, along with Congress, must always weigh in should passenger security or privacy be compromised. In a competitive environment, companies like Unisys can facilitate the expansion of a Registered Traveler program, bringing the best solutions and utilizing the most effective technology in the most cost-efficient manner.

Thank you again for the opportunity to testify before you today. Unisys looks forward to assisting government agencies and lawmakers as they continue down a path where security is at the forefront of many of its decisions. I am happy to answer any questions you might have.

Mr. ROGERS. Thank you for your statement, Mr. Zmuda.

The chair now recognizes Mr. Marc Rotenberg, Executive Director of the Electronic Privacy Infrastructure Center, for his statement.

The floor is yours.

STATEMENT OF MARC ROTENBERG

Mr. ROTENBERG. Thank you very much, Mr. Chairman, members of the committee. I appreciate the opportunity to participate in the hearing today and also the attention that you are giving to the privacy issue.

As you know, this has been a critical concern in previous programs involving airline passenger screening. And we think it will be a critical issue to evaluate Registered Traveler.

Since your last hearing was held, EPIC obtained documents under the Federal Freedom of Information Act which revealed a series of errors on the watch list. These are documents that were provided to us by the TSA.

We have over 100 instances which show circumstances where people were placed on the watch list. They believe, of course, that those determinations were made in error.

The problem here is that that information is the basis for the Registered Traveler program. And although Mr. Hawley described a redress procedure earlier, it is not clear how that redress procedure will fix the problems for travelers who are pulled aside and told that they are placed on the watch list.

Now, part of the reason that this happens, we believe, is because the type of privacy protections that apply to other information held by the federal government do not apply when we are talking about programs like Registered Traveler. You do not have the right to get access to the information or to challenge a determination that has placed you on a watch list.

Now, let's think about this in very practical terms. We have privacy laws in the private sector, for example, that require, when you apply for a car loan or a home mortgage, if the financial institution turns you down, you are shown the basis for that determination.

And not surprisingly, a lot of times people are turned down for loans because of inaccurate information, because names are confused, because information is outdated.

The key point here I would like to make is that privacy is not simply about limiting who has access to information. It is about ensuring accuracy and accountability. And the reason that privacy laws typically give people the ability to inspect the information about them when a decision is made about them is to ensure that an accurate decision is made.

Now, you are proceeding with a program right now where determinations will be made about people. And they will be turned down. And they will not be given the opportunity to challenge that determination.

You may assume that it will not be so difficult for members of Congress to be cleared for Registered Traveler approval, but I suspect that many of your constituents are going to run into a lot of trouble and a lot of frustration.

There is a third point I would like to make, as well, and that is that there is clearly a risk with this program, particularly if it is pursued in the private sector, for mission creep. Now, as you know, this has also been an issue with the passenger screening programs.

There is no dispute about the need to keep terrorists and, you know, anybody who intends harm against the United States or air travel safety off planes, no dispute whatsoever.

But, of course, as the data has been collected on air travelers, a whole range of other applications have been considered, wanted fugitives, criminal offenders, outstanding warrants, misdemeanors. The list became quite long. And it was the length of the list, in part, which led to the demise of the CAPPS II program.

We agree with the current focus of the TSA, which is to keep those people who are considered to be terrorists off planes. The question is: How far will this program go if, as Mr. Brill proposes, it is used for other applications, access to sports stadiums, access to federal office buildings, access to apartment buildings in midtown Manhattan?

The type of threat assessment in those scenarios is very different, frankly, from the type of threat assessment that the TSA might make, regarding whether a person should board a commercial airline in the United States.

So we think three things should happen before the program goes forward. First, there has to be a means to fix the watch list. You simply cannot rely on data that is going to have errors in it and that is going to wrongly place American citizens, essentially, on a blacklist, where they will be stigmatized and prevented from boarding planes.

Second, we think something like the Privacy Act needs to apply, not only to this records system, but certainly to any similar records system that might be operated in the private sector. And if Mr. Brill's program goes forward, or the Unisys program goes forward, there have to be legal restrictions on how that data is used.

And finally, we urge you—urge you—to limit the use of this data for the determination about who boards an airline in the United States. This should not become an open-ended program of trying to decide who belongs on a list of favorite Americans and who ends up on a list of disfavored Americans.

I do not think that was ever the intent, but oftentimes these programs evolve. And now is the opportunity to make clear what the endpoint will be.

So thank you for giving me this opportunity.

[The information follows:]

Prepared Statement of Marc Rotenberg

Mr. Chairman, Members of the Committee, thank you for the opportunity to appear before you today. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are very pleased that the Committee is examining the privacy implications of the Registered Traveler program. I ask that my complete statement, EPIC's recent report on Registered Traveler, and our one-page summary of the ongoing problems with watch list errors be entered into the hearing record.[1]

[1] EPIC, *Spotlight on Surveillance: Registered Traveler: A Privatized Passenger ID* (October 2005), available at http://www.epic.org/privacy/surveillance/spotlight/1005/default.html

ELECTRONIC PRIVACY INFORMATION CENTER

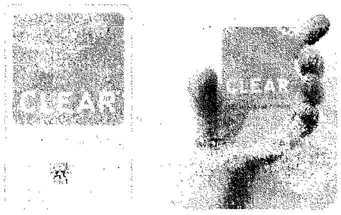
Spotlight on Surveillance

October 2005:

Registered Traveler Card: A Privatized Passenger ID

The federal government is spending an increasing amount of money on surveillance technology and programs at the expense of other projects. EPIC's "Spotlight on Surveillance" project scrutinizes these surveillance programs. For more information, see previous Spotlights on Surveillance.

This month, Spotlight focuses on the Transportation Security Administration's Registered Traveler program. The government pilot program began a year ago and recently ended at five airports; however, a private business is continuing the program at Orlando International Airport and there are plans to expand the air traveler prescreening program to many airports across the nation.[1]



View a list of requirements to obtain a Clear Registered Traveler card.

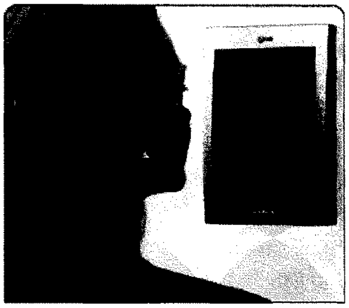
Source: Clear Registered Traveler http://www.flyclear.com

The government has spent about $20 million on the pilot Registered Traveler program.[2] The federal test program ended last month when Fiscal Year 2005 ended because no money has been allotted toward the program in the Fiscal Year 2006 budget.[3] However, the Transportation Security Administration (TSA) continues to conduct background checks on applicants and members of the private program, named Clear and operated by Verified Identity Pass Inc., at a cost of $30 to $50 per check, paid for by TSA.[4]

From July 2005 (the beginning of the privately run Clear program at Orlando airport) to September 2005, about 8,600 people have joined Clear.[5] The applicant, who must be a U.S. citizen or permanent foreign national, pays an annual fee of $79.95 to join.[6] To apply, the applicant first completes a form that asks for biographical information including: previous home addresses for the past five years, Social Security number,[7] Alien Registration Number and date of arrival in the United States (if applicable), and driver's license number.[8] Once the applicant completes the form, he must go to a ClearSpace Enrollment Station (as of now, only located at Orlando International Airport). The applicant must bring two forms of identification, one of which must be a photo ID. The acceptable identification documents include unexpired U.S. passport; military, voter registration or Social Security cards; unexpired driver's license; or original or certified birth certificate.[9] Clear then says that:

We carefully examine these documents for authenticity using the latest document inspection technology to detect tampering or counterfeiting. So that we have a complete record of your application, we store in a separate, secure database the biographical information and an image of the documents you submit to enroll.[10]

The applicant then submits digital images of his fingerprints and iris, and a digital photo. Clear then "create[s] and store[s] a template, or mathematical representation, of the finger and iris images, to create a unique biometric ID of the Member."[11] Then, all of the data submitted by the applicant is sent to TSA, which then creates the applicant's "security threat assessment" based upon a background check that includes its controversial "no-fly lists."[12] TSA continues to conduct security reviews of Clear members throughout their membership, and if a person's security threat assessment changes from approved to unapproved, the person is informed and their Clear membership discontinued.[13] A rejected applicant cannot appeal this decision, and TSA will not disclose any information as to why the person was rejected.[14]



Applicants to the Clear Registered Traveler program must submit both iris and fingerprint scans.

[click to view full brochure in pdf]

Source: Iridian Technologies
http://www.iridiantech.com

Significant privacy and security risks are inherent in this Registered Traveler program. First, there is a substantial security risk as the divides travelers into categories whose criteria can be learned and exploited. Second, there is a privacy risk because the program's members will not have the protections of the Privacy Act of 1974, as only government agencies are subject to the law. Third, the program has a risk of mission creep – a risk that information volunteered will be used for reasons not related to their original aviation security purposes.

First, the program creates two classes of travelers: trusted and not trusted. But, as security expert Bruce Schneier has explained, this program also creates a third category: "bad guys with the card."[15] Criminals will choose applicants without previous links to terrorism, who can pass the background checks, to commit their crimes.[16] (Schneier also has noted that, because Clear discontinues the membership of anyone who fails the continuous TSA security review, potential terrorists can pay $80 per year to "be automatically notified if the Department of Homeland Security is onto him.")[17]

Airports that have joined the Registered Traveler Interoperability Consortium:

1. Albany International Airport
2. Atlantic City International Airport
3. Bangor International Airport
4. Blue Grass Airport
5. Boston Logan International Airport
6. Chattanooga Metropolitan Airport Authority
7. Dallas Fort Worth International Airport *
8. Denver International Airport *
9. Dickinson Theodore Roosevelt Regional Airport
10. Flagstaff Pulliam Airport
11. Fort Wayne International Airport
12. Ft. Lauderdale-Hollywood Int'l Airport
13. Grand Forks Regional Airport Authority

Second, the private company would be in charge of verifying identity documents and maintaining a database full of personally identifiable data and images of the identity documents submitted by U.S. citizens and permanent foreign residents. The private company, unlike TSA and other federal government agencies, is not subject to the restrictions of the Privacy Act of 1974.[18] When passing the Privacy Act, Congress sought to restrict amount

Greater Orlando Aviation Authority
15. Greater Rockford Airport Authority
16. Jackson Hole Airport
17. Kent County Department of Aeronautics
18. Lafayette Regional Airport
19. Lambert-St. Louis International Airport
20. Lihue Airport
21. Metropolitan Knoxville Airport Authority
22. Metropolitan Nashville Airport Authority
23. Mid-Ohio Valley Regional Airport
24. Minneapolis St. Paul International Airport *
25. Monterey Peninsula Airport
26. Myrtle Beach International Airport
27. Northwest Arkansas Regional Airport
28. Northwestern Regional Airport Commission
29. Palm Beach International Airport
30. Palm Springs International Airport
31. Peninsula Airport Commission
32. Philadelphia International Airport
33. Phoenix Sky Harbor *
34. Pittsburgh Int'l Airport-Allegheny County Airport Authority
35. Port Columbus International Airport *
36. Port Of Seattle/Sea-Tac Int'l Airport
37. Pullman-Moscow Regional Airport
38. Redmond Airport
39. Reno Tahoe Airport Authority
40. Rhode Island Airport Corporation
41. Roanoke Regional Airport Commission
42. San Francisco International Airport *
43. Santa Barbara Airport
44. Shenandoah Valley Regional Airport
45. Washington Authority's Reagan Washington National and Dulles International Airports *
46. Tucson Airport Authority
47. Tupelo Regional Airport
48. Waco Regional Airport
49. Wayne County Airport Authority
50. Wilmington International Airport
51. Yeager Airport

* denotes a founding member

Source: Registered Traveler Interoperability Consortium *http://rtconsortium.org*

of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[19] The members of the Clear Registered Traveler program would be subject to the private company's choice of what data to collect, how and where to store the data, and who has access to the data.

The information would not necessarily have stringent privacy protections when transmitted to TSA, however. TSA exempted the Registered Traveler records system from many protections the Privacy Act is intended to provide.[20] TSA's notice leaves it under no legal obligation to inform the public of the categories of information contained in the system or provide the ability to access and correct records that are irrelevant, untimely or incomplete.

"Member[s] can request a copy of everything that Verified ID and its subcontractors have in their information systems files for the Clear Program identified to the Member personally, and Verified ID and its subcontractors will provide this information," according to the Clear program.[21] However, TSA conducts a "Security Threat Assessment" of all applicants to determine if they can join the Clear program, and the reasons behind a positive or negative Security Threat Assessment are not communicated to applicants or the Clear program.[22] Applicants cannot appeal such assessments by TSA.[23]

The lack of access and correction is especially troubling in light of the fact that documents recently obtained by EPIC under the Freedom of Information Act show nearly a hundred complaints from airline passengers between November 2003 and May 2004 about the government's traveler screening security measures.[24] The most common complaint from travelers is that they have been wrongly placed on a government watch list.[25] The Transportation Security Administration maintains "selectee" and "no fly" watch lists of individuals suspected of posing a risk to air travel safety. When a passenger checks in for a flight, he may be labeled a threat if his name matches an entry on one of the watch lists, even if he is not the person actually on the list. People who are identified as watch list matches may experience long screening delays or not be allowed to board the plane.

TSA maintains that it has an adequate redress process to clear individuals improperly matched to watch lists; however, it is well known that individuals encounter difficulty in resolving such problems. Senators Ted Kennedy (D-MA) and Don Young (R-AK) are among the individuals who have been improperly flagged by watch lists.[26] Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge; unfortunately, most people do not have that option. A clear, timely, access and correction procedure is vital for the Clear Registered Traveler program. The watch-list complaints show that mistakes are made that significantly affect innocent Americans. As of now, Registered Traveler applicants who receive a negative Security Threat Assessment do not even have the redress process offered to those incorrectly matched to watch lists.

TSA also has recently been criticized for its administration of the test passenger prescreening program, Secure Flight, which is similar to Registered Traveler. The agency began testing the Secure Flight system earlier this year. In June, however, TSA admitted that it had collected and maintained detailed commercial data about thousands of travelers in violation of a notice published last fall stating it would not do so.[27] In July, the Government Accountability Office (GAO) concluded that these actions violated the Privacy Act.[28] According to the GAO letter, "the agency did not provide appropriate disclosure about its collection, use and storage of personal information as required by the Privacy Act," and "[a]s a result of TSA's actions, the public did not receive the full protections" of the law.[29] Stringent privacy protections are necessary, and it has been shown that travelers' rights are not secure even when the program is administered by a federal agency subject to privacy laws. The privacy rights of travelers would receive far less legal protection under a program administered by a private company not subject to the Privacy Act of 1974.

A third risk associated with the Clear and federal Registered Traveler program is that of mission creep. Program applicants must submit a substantial amount of personally identifiable information that Clear keeps – including biometric data and digital images of identity documents, such as birth certificates, Social Security cards, and driver's licenses. It is possible for Clear program members to be tracked, because Clear "will maintain 'log files' of entrances to local venues."[30] The company states that it keeps the log files only at the local venue and these files are automatically purged every 24-48 hours.[31] However, the possibility for easily tracking travelers is there, and it would be tempting to use the excuse that "homeland security" and "terrorism prevention" demand that such tracking be done.

In the past, TSA has exhibited a proclivity for using personal information for reasons other than the ones for which the information was gathered or volunteered. Though TSA has stated that it will not use the sensitive personal data of tens of millions of Americans for non-aviation security purposes, TSA documents about another passenger prescreening program similar to Registered Traveler, the CAPPS II program, collected by EPIC under the FOIA clearly show that TSA had considered using personal information gathered for CAPPS II for reasons beyond its original purposes. For example, TSA stated that CAPPS II personal data might be disclosed to federal, state, local, foreign, or international agencies for their investigations of statute, rule, regulation or order violations.[32]

In the case of Registered Traveler, TSA has identified thirteen categories of "routine uses" of personal information that will be collected and maintained in the program's system of records. In one category, TSA anticipates disclosure to "the appropriate Federal, State, local, tribal, territorial, foreign or international agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where TSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation."[33] This category is so broad as to be almost meaningless, allowing for potential disclosure to virtually any government agency worldwide for a vast array of actual or "potential" undefined violations.

Beyond the above mission creep possibilities, there are the comments made by Steven Brill, who runs the Clear program's parent company Verified Identity Pass Inc. Brill has said that he envisions the Clear card becoming more than just an aviation security ID card. Brill's company has partnered with rental car company Hertz and online travel booking company Orbitz to market the Clear program cards, and is expected to announce a partnership with an airline soon.[34] Brill has said that he hopes the Clear ID card would also be used at office buildings, power plants and stadiums.[35] The development of such an unregulated ID system has significant implications for Americans. Entry into an office building or stadium should not be conditioned upon whether the person can afford a privatized ID card.

---

[1] The pilot program was launched by the Transportation Security Administration at six airports in Boston, Houston, Los Angeles, Minneapolis, and Washington, DC. To date the only privately run Registered Traveler program is at Orlando International Airport, but the Registered Traveler Interoperability Consortium hopes to deploy private Registered Traveler programs at 50 airports around the nation. Thomas Frank, *Biometric IDs could see massive growth*, USA Today, Aug. 15, 2005; Registered Traveler Interoperability Consortium *at* http://www.rtconsortium.org.

[2] Department of Homeland Security, *Budget-in-Brief Fiscal Year 2006*, at 21 (Feb. 7, 2005) *available at* http://www.epic.org/privacy/surveillance/spotlight/0505/dhsb06.pdf.

[3] Bruce Mohl, *They Pay to Ease Security*, Boston Globe, Aug. 7, 2005.

[4] Thomas Frank, *Biometric IDs could see massive growth*, USA Today, Aug. 15, 2005.

[5] Jerry W. Jackson, *Privately run traveler program to stay at OIA*, Orlando Sentinel, Sept. 28, 2005.

[6] Clear Registered Traveler *at* http://flyclear.com/.

[7] Clear states that the applicant does not have to submit his Social Security Number, but "the absence of this data may delay or prevent the completion of the security assessment, without which the applicant may not be permitted to participate in this program." *Id.*

[8] *Id.*

[9] *Id.*

[10] Clear Registered Traveler, *supra* note 6.

[11] The Clear program's subcontractors include Lockheed Martin Corp and Iridian Technologies Inc. *Id.*

[12] *Id.*

[13] *Id.*

[14] Clear Registered Traveler, *supra* note 6.

[15] Bruce Schneier, *Crypto-Gram Newsletter*, Mar. 15, 2004 *available at* http://www.schneier.com/crypto-gram-0403.html.

[16] Neither Oklahoma City bomber Timothy McVeigh nor Unabomber Ted Kaczynski had previous ties to terrorism, Schneier said. *Id.*

[17] Bruce Schneier, *Crypto-Gram Newsletter*, Aug.15, 2005 *available at* http://www.schneier.com/crypto-gram-0508.html.

[18] 5 U.S.C. § 552a (1974).

[19] S. Rep. No. 93-1183, at 1 (1974).

[20] Privacy Act Notice, 69 Fed. Reg. 54256 (Sept. 8, 2004).

[21] Clear Registered Traveler, *supra* note 6.

[22] *Id.*

[23] *Id.*

[24] Department of Homeland Security, Transportation Security Administration, *Complaint Log*, November 2003 to May 2004, obtained by EPIC through FOIA litigation, *available at* http://www.epic.org/privacy/airtravel/foia/complaint_log.pdf.

[25] *Id.*

[26] *See, e.g.*, Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Washington Post, Sept. 30, 3004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press International, Aug. 20, 2004.

[27] Privacy Act Notice, 70 Fed. Reg. 36,320 (June 22, 2005) *available at* http://www.epic.org/privacy/airtravel/sf_sorn_pia_062205.pdf.

[28] Government Accountability Office, Letter to Congressional Committees, July 22, 2005 *available at* http://www.epic.org/privacy/airtravel/d05864r.pdf.

[29] *Id.* at 2, 4.

[30] Clear Registered Traveler, *supra* note 6.

[31] *Id.*

[32] Transportation Security Administration, Department of Homeland Security, *Draft Privacy Impact Statements (CAPPS II)*, April 17, 2003, July 29, 2003, and July 30, 2003, obtained by EPIC through FOIA litigation, *available at* http://www.epic.org/privacy/airtravel/profiling.html.

[33] Privacy Act Notice, 69 Fed. Reg. 30948, 30950 (June 1, 2004).

[34] Laura Meckler, *Air Security: Shorter Waits For More Fliers?*, Wall Street Journal, Sept. 28, 2005.

[35] Brian Bergstein, *Voluntary Security ID to Debut in Florida*, Associated Press, June 3, 2005.

EPIC Spotlight on Surveillance Page | EPIC Privacy Page | EPIC Home Page

In my statement today, I wish to call attention to three particular problems with the Registered Traveler program. First, the security watch lists on which the system is based are filled with inaccurate data. Documents obtained by EPIC under the Freedom of Information Act reveal that travelers continue to struggle with watch list errors.[2]

[2] EPIC FOIA Notes, "Travelers Continue to Struggle with Watch list Errors," No. 8 (Sept. 27, 2005) available at http://www.epic.org/foia__notes/note8.html

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

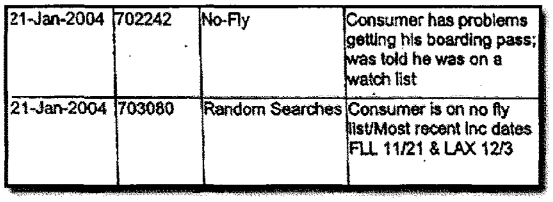
FOIA notes

EPIC FOIA Notes #8

September 27, 2005

TRAVELERS CONTINUE TO STRUGGLE WITH WRONGFUL WATCH LIST MATCHES

SNAPSHOT [CLICK FOR FULL DOCUMENT—pdf, 2.2mb]



21-Jan-2004	702242	No-Fly	Consumer has problems getting his boarding pass; was told he was on a watch list
21-Jan-2004	703080	Random Searches	Consumer is on no fly list/Most recent Inc dates FLL 11/21 & LAX 12/3

THE DISCLOSURE

Documents obtained by EPIC from the Transportation Security Administration under the Freedom of Information Act reveal nearly a hundred complaints from airline passengers between November 2003 and May 2004. The most common complaint from passengers is that they have been wrongly placed on a government watch list. Numerous complaints show passengers' frustration with the agency's failure to resolve their misidentification problems.

THE ISSUE

Watch list accuracy and redress rights of American travelers.

THE BACKGROUND

The Transportation Security Administration, which is part of the Department of Homeland Security, maintains "selectee" and "no fly" watch lists of individuals suspected of posing a risk to air travel safety. When a passenger checks in for a flight, he may be improperly labeled a threat if his name matches an entry on one of the watch lists—even if he is not the person on the list. People who are identified as watch list matches may experience long screening delays or not be allowed to board the plane.

THE SIGNIFICANCE

The government has not solved the problems that lead airline passengers to be wrongly labelled as as watch list matches, and innocent individuals still have a hard time clearing their names.

About the Freedom of Information Act

The Freedom of Information Act establishes a legal right for individuals to obtain records in the possession of government agencies. The FOIA is critical for the functioning of democratic government because it helps ensure that the public is fully informed about matters of public concern. The FOIA has helped uncover fraud, waste, and abuse in the federal government. It has become particularly important in the last few years as the government has tried to keep more of its activities secret.

EPIC FOIA Notes

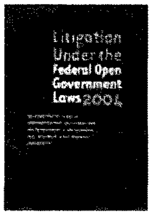
Subscribe / Unsubscribe

Contact: +1 202 483 1140 x224 (FOIA Notes Hotline)

FOIA Links

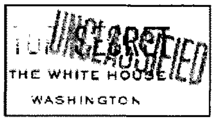
EPIC Open Government
EPIC 2005 FOIA Gallery
National FOI Day
FOIA Advocates Network
PI FOIA Project
Open the Government
Freedominfo.org
Secrecy News

FOIA Publications



Litigation Under the Federal Open Government Laws 2004

FOIA Documents



UNCLASSIFIED
THE WHITE HOUSE
WASHINGTON

A second flaw in the program exacerbates this problem—the databases in the system are currently not subject to the full safeguards of the Privacy Act of 1974, as the TSA has sought wide-ranging exemptions for the record system and private companies are not generally subject to the Privacy Act. As a result, the legal safeguards that help ensure accuracy and accountability are simply missing from this system.

Third, the Registered Traveler program, if operated in the private sector, will become a textbook example of "mission creep"—the databases of personal information will be used for purposes other than aviation security.[3] We already know that the Computer Assisted Passenger Prescreening System 2 ("CAPPS 2"), the precursor to Registered Traveler, was to be used for purposes unrelated to terrorist screening. Because of this, Congress rightly chose to end the program.[4] This danger is even more "clear" with the Registered Traveler program, now under consideration by the Committee.

Last month, the federal government ended the test program for Registered Traveler.[5] Before the program goes forward, at least these three issues should be addressed.

TSA's Watch List Errors

The Registered Traveler system is based on the TSA's existing system of passenger screening lists. These same lists have been a constant source of errors and inaccuracies that inappropriately detain travelers, subject them to unnecessary searches, and sometimes prevent them from flying.

Senators Ted Kennedy and Don Young, for instance, have both been improperly placed on security watch lists. In hearings before this Subcommittee in March, Ranking Member Sanchez noted that many of her constituents had experienced unwarranted delays, questioning, and sometimes even the inability to fly, due to their names being mistakenly placed on screening lists.

Hundreds of other passengers have experienced the same or similar problems. Documents received by EPIC through the Freedom of Information Act revealed that, in the period from November 2003 to May 2004, over a hundred individuals complained of being placed on the lists in error.

Nor is removal from the watchlists a simple matter. Senator Kennedy was only able to correct this error after appealing directly to then-Homeland Security Secretary Tom Ridge. The vast majority of people affected by watchlist errors, needless to say, do not have this option. Instead, they face an opaque and arbitrary bureaucratic process, where they are never told the reasons for their being placed on the lists, and therefore have little idea how to correct false information about themselves or distinguish themselves from a suspect with a similar name.[6]

The provisions surrounding Registered Traveler databases are no better. Although Verified ID claims that "members" of the program will be provided with the identification information in the private database, the most pertinent information will not be revealed to those people who provide information to the Registered Traveler system.[7]

For instance, if an applicant is denied membership, or if a member's status on the watch lists changes, the individual is never told why he has been deemed a potential security risk. Furthermore, applicants who have supplied sensitive personal information to the program are not assured of access to the information that the system has on them, and therefore have no way of ensuring either the accuracy or the security of their data.

Lack of Privacy Act Safeguards

These problems are all the more serious because the Registered Traveler system is not subject to most of the critical privacy safeguards required by the Privacy Act of 1974. Congress passed the Privacy Act in response to concerns that the rapid growth of government databases could have negative effects on the personal privacy and civil rights of citizens. After intensive study, extensive hearings, and careful consideration, Congress adopted the Privacy, Act, which requires government agen-

[3] Systems designed to protect the country from terrorist acts are increasingly being used for many other purposes. Barry Newman, "New Dragnet: How Tools of War on Terror Ensnare Wanted Citizens: Border Immigration Officials Tap Into FBI Databases; Questions About Privacy," Wall Street J., Oct. 31, 2005, at A1.

[4] Matthew Wald & John Schwartz, "Screening Plans Went Beyond Terrorism: Air security program sank after it grew to include other needs," N.Y. Times, Sept. 19, 2004, at A25.

[5] Sara Kehaulani Goo, "Registered Traveler Test is Ending Inconclusively: Airport Security Scheme Lacks Broad Support," Wash. Post, Sept. 27 at A15.

[6] The issue of redress procedures was considered in a 2004 report on Registered Traveler, but never resolved. Transportation Security Administration, *Registered Traveler Pilot: Privacy Impact Assessment 6* (June 24, 2004).

[7] Clear Registered Traveler at http://flyclear.com/

cies to limit the collection, sharing, and use of individuals' personal information. The Act also requires that agencies give individuals the right to access, and correct, information that the government collects about them.

For all practical purposes, the Registered Traveler Program withholds these rights from individuals. In this case, we have two separate databases, each of which sidesteps Privacy Act responsibilities.

In the case of a private partner, the data collected from passengers is stored in a separate, private database. As a private entity, the partner is not covered by any of the requirements of the Privacy Act. When TSA says that its contractors must abide by the Privacy Act, this is only with regard to the information flowing from the TSA to the contractor, not for this separate, private database of personal information collected and kept by the private company. Thus, the only guarantee of privacy that passengers have comes from the company's own broad assurances.

In removing Privacy Act safeguards from the private-sector database, applicants are not only denied the ability to access and correct records, they also are subject to the sharing of their personal information. The data collected from applicants includes some of the most sensitive information that one can collect about a person: Social Security numbers, fingerprint and iris scans, photographic reproductions of drivers licenses, passports, and birth certificates. This information requires limits on its use and sharing mandated by law. Registered Traveler evades this responsibility by having passengers initially submit data to private partners.

The privacy policy of Verified ID states that data is shared only with the TSA, and no other agencies. Yet a look at the Privacy Act notice by the TSA quickly reveals that TSA is prepared to share passengers' personal information with a wide array of other agencies, whether federal, state, local, international, or foreign. The standards for this sharing are alarmingly low—the TSA must be aware only of an *indication* of a *potential* violation of civil or criminal laws or *regulations.*

The TSA's own database, which does fall under the scope of the Privacy Act, does little more than give a cursory nod to its requirements. TSA has exempted itself from the Privacy Act's requirements for accounting for disclosures, access to records, and even the requirement that the information in the database be *necessary* and *relevant.*

By exempting Registered Traveler from the access to records requirements, TSA prevents users from requesting any information that the TSA may be keeping on them. As I have already noted, this access requirement is crucial in any system that is to respect the rights of individuals. Without meaningful access to the files kept on them, individuals have no recourse if inaccurate, incomplete, or fraudulent information about them is kept in the system. A person with a faulty file will not only lack the opportunity to correct it, she will never learn that it is faulty in the first place, and be unable to clear her name.

It is significant that the Department of Homeland Security Data Privacy and Integrity Advisory Committee recently prepared a report on the use of commercial data for passenger screening and recommended strict limitations on the use of commercial data for passenger screening.[8] As the Committee noted, "False positives can create adverse consequences for misidentified individuals, ranging from missing a flight to being denied a security clearance or a job."[9]

There is also ample precedent for imposing privacy obligations on the private sector. Consider determinations that are made by banks and other financial institutions about a consumer who seeks a home loan. If a loan application is denied, the consumer is entitled to know the basis for the decision. The reason, not surprisingly, is that mistakes are made, names are confused, incorrect data is used, information is transposed, unsubstantiated allegations are left unchallenged.

A watch list system is necessarily open to such abuse and any benefits that might result must be weighed against the very real harms to innocent individuals. A privatized watch list system opens the door to the routine stigmatization of a large percentage of the American public with no effective means of redress.

"Mission Creep"

The breadth and scope of the information to be kept in the Registered Traveler data base leads to another significant concern—that this program will begin to accumulate other uses for which it was not originally approved or intended. Such "mission creep" leads to further privacy risks.

[8] Report of the Department of Homeland Security Data Privacy and Integrity Advisory Committee, *The Use of Commercial Data to Reduce False Positives in Screening Programs* (Sept. 28, 2005).

[9] *Id.* at 2.

Mr. Brill has suggested that his identification component of the program be used not only in airports, but also as a means to control access to sports arenas, power plants, and even office buildings. Just this week Mr. Brill announced that his company had entered into agreements with Hertz, the rental car industry leader, and Cendent, an Internet management travel company.[10]

Should those who rent cars or book air travel on the Internet be concerned that if they do not first get Mr. Brill's gold star, they may soon face higher prices for travel or additional questions from the rental company? And what about people who travel infrequently, or whose personal information may be more difficult to verify? Database errors also tend to fall disproportionately on minority communities and those whose names are easily misspelled or mispronounced.

The TSA has indicated that it will combine Registered Traveler with at least six other databases under the office of Screening Coordination and Operations. The agency has not specified how it intends to protect privacy rights in this amalgam of databases. If a person provides personal information to an agency for a specific purpose, he generally expects the agency to limit its use of the information to that purpose.

The risks of mission creep are not theoretical. The TSA has itself suffered from this problem, as indicated by its misuse of passenger data in the CAPPS II program. TSA documents obtained by EPIC under the Freedom of information Act clearly showed that TSA has considered using information gathered for the CAPPS II program for reasons beyond its original purposes. For example, TSA stated that CAPPS II personal data might be disclosed to federal, state, local foreign, or international agencies for their investigations of statute, rule, regulation, or order violations. Congress rightly put an end to that program.[11]

But at least that program was limited to law enforcement conduct. There appear to be no "clear" limits to Registered Traveler.

Recommendations

The privacy of individuals in the United States is a fundamental right that should not be sacrificed for mere convenience. In protecting these rights, I urge you to consider the following:

1. The TSA watch lists have widespread problems, flagging as security risks a minimum of hundreds of passengers who pose no threat. A system based around these watch lists and integrated with other systems of records will only exacerbate the problems that have been well documented.

2. The Privacy Act creates critical and necessary safeguards not simply to protect privacy, but also to ensure accuracy and accountability. Any government-approved security system that keeps personal information on individuals should meet the Privacy Act requirements for necessity, relevance, and openness, including individual access and correction. It should be made clear that these requirements apply whether the information originates with the agency or with information provided by the individual. It should also not be subject to broad exceptions like those the TSA has set forth in its notices.

3. There are real risks in a database accumulating unintended uses with unforeseen consequences. The end result is often an unwieldy tool that performs poorly, operates inefficiently, and violates privacy. I urge you to mandate any system designed for aviation security be restricted to that purpose, and not become a system for tracking individuals or controlling their ability to travel in going about their daily business.

Congress was wise to discontinue the Registered Traveler program last month. The program should not go forward until these problems are resolved.

Thank you for the opportunity to appear here today. I will be pleased to answer your questions.

Mr. ROGERS. I thank all of you for your statements. Those were very thought-provoking.

And we will start now with the chairman of the subcommittee for any questions that he may have.

Mr. LUNGREN. Thank you very much.

[10] Verified Identity Pass, Inc., "Press Release," (Nov. 1, 2005) available at http://www.verifiedidpass.com/news__pr__110105.html

[11] Former Secretary of Homeland Security Tom Ridge acknowledged that the CAPPS 2 program was "dead" in mid-2004. Ryan Singel, "Passenger Screening System Dead," Wired (July 15, 2004), available at http://www.wired.com/news/privacy/0,1848,64227,00.html.

Mr. Barclay, there is some discussion about the clearinghouse in questions asked of Mr. Hawley. And very, very quickly, as I understand, the clearinghouse is merely a mechanism which takes the information that you would get from a private vendor and basically bundles it up to send it to the government agency that does the background check, and then you receive the information back and distribute it to the private vendors.

Is that correct?

Mr. BARCLAY. Correct.

Mr. LUNGREN. And the price that you charge for that is what?

Mr. BARCLAY. Well, the price currently for the employee checks, which do not have—it is just one way going in—

Mr. LUNGREN. Right.

Mr. BARCLAY. —is $7. And that includes the fees for the basic background vetting, that was started with just a criminal history record check. And then there was added a number of other checks, including what was ONRA at the time.

And some other services were added, as time went on, to take it from $4 to $7. And that is for the fee that relates to the $29 currently—for criminal history record checks of employees.

The passenger checks—we have been told, again, that this is a clearinghouse that is in a nonprofit, that is owned by airports, and airports are the customers and the owners. So they are watching. And they have told this organization to be cost-based.

So, over time, those fees probably go down. Well, they will go down with volume. The issue there is not a per-fee cost. It is what is the volume and what are the costs of doing—

Mr. LUNGREN. What limitation, other than your good graces, is there on setting a higher fee?

Mr. BARCLAY. The fact that the customers and the owners are the same people and their public agencies, trying to just get a cost-based process.

Mr. LUNGREN. But your true customer in this would be the passenger. And the passenger would purchase this right, or purchase this card, through a private vendor. The private vendor would have to go through you.

If you are the exclusive mechanism by which they can go through this, what—I mean, I think this is the concern some people have—What limits do we have on you?

Mr. BARCLAY. The airports are going to be putting out bids to collect them from the private vendors, which will include, what will the price be at each airport? So that is part of the cost-based analysis.

I mean, there is no incentive for a nonprofit organization who are the customers, who are the airports that are going to be deciding what the fee is that goes to the clearinghouse, and they are the owners. There is a great deal of transparency here.

So there is just no incentive to charge more than what it costs—

Mr. DICKS. Would the chairman yield just for a point?

Mr. LUNGREN. I will be happy to. I have to go back down to cast another vote, so I will happily yield my time to the gentleman. But I will be back.

Mr. DICKS. Wouldn't there also be—there would be an elastic curve here. I mean, hike the fee up too high, people are not going to sign up.

Mr. BARCLAY. Well, as Mr. Brill said, the fee—if you have different fees at different airports, as a result of the bidding process, that is going to help keep the fee down, because you know, in Dallas, putting out your plan is competing with folks who can sign up in Boston while they are up there, if it is a lot cheaper.

So there is going to be a regulating effect. But the job of the clearinghouse specifically is exactly the same as it is for employees.

We have already done, again, 1.8 million record checks. It is working very smoothly. Our fees are much lower than they are for truckers and others in the business.

So I would argue there is no evidence that there is an incentive there. And the structure does not have an incentive.

Mr. ROGERS. The chair now recognizes the ranking member of the full committee, Mr. Thompson, for any questions he may have.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Just to elaborate a little more with Mr. Barclay on that, you have testified that the clearinghouse process is cost-based.

Mr. BARCLAY. Yes, sir.

Mr. THOMPSON. And I am assuming that, because of that, there is no profit associated with what you do?

Mr. BARCLAY. Right. We go for fully allocated costs for what we do, and that is true of the current process for employees. And we have been told by our owners, the airports, to make it true for any future process, such as Registered Traveler.

Mr. THOMPSON. Okay. And I guess the part of the question is, how do you see us keeping the Registered Traveler program a security program and not a perks program?

Because we have heard testimony in the past that?or business people will jump at something like this, and I think the effort that I hear the committee talks about, we want to make sure the traveling public is secure and not that they can pick up another card and travel through the airport.

Mr. BARCLAY. No, and that is what everyone is struggling with a little bit. You have got a program that has to have elements of the private industry for marketing and other services that need to be provided, local government in airports that are there.

And airports have the same incentives as the federal government. They want this program to be both a security program and a convenience program.

And then the federal government that is focused primarily on the security aspect of this, because it is TSA doing it. And you have got to come up with a plan that merges all those different incentives.

I think the thing you key on for security, again, is what I said in my testimony, that you have a very small number of people who are traveling for a living, getting on and off airports constantly. If you can know a lot about them—they make up such a high percentage of the travelers—you can apply a lot more of your limited resources on the people you do not know anything about.

That helps both lines. The Registered Traveler line will move real fast. The other line will move faster because you do not have those registered travelers in it who are making up a large percentage of the passengers.

Mr. THOMPSON. Thank you.

Mr. Brill, you provided an explanation of wait time associated with Orlando Airport. Can you tell me, on an average, how many passengers go through the Orlando Airport on a daily basis?

Mr. BRILL. The number of all passengers or our passengers?

Mr. THOMPSON. All passengers.

Mr. BRILL. I just do not know that.

Mr. THOMPSON. Well, I guess it would help us make a real objective analysis of—

Mr. BRILL. We can provide that for you. I am about to guess at an annual number, and I am going to get into trouble, so I will not.

Mr. THOMPSON. Well, let me give you an example. You say that non–Registered Traveler people wait time is 31 minutes. Under your program, it is three minutes, with an average of 4 seconds?

Mr. BRILL. I do not want to get into trouble with my friends at the airport. In the days that we have observed since we have been there, the maximum wait time—and it has happened a lot—during the busy hours has been as much as 31 minutes.

I do not want to generalize, because I know we do not say that that is the average wait time. But there is a dramatic difference, yes.

Mr. THOMPSON. We need to be able to put some numbers to what you shared with us, because you say your average Registered Traveler traveling is 165 individuals a day.

Mr. BRILL. That is right. That is for the first 45 days of the program. That number—and I think there is a footnote there; I do not have it in front of me—is going up everyday.

That is when we had 3,000 or 4,000 members. We now have 10,000. I was in Orlando on Tuesday morning. And I think we had 350 people go through by 10, 10:30 in the morning, through our—

Mr. THOMPSON. Well, what I am trying to get at is, that 165 per day you gave us if of how many people who travel in day. Is that of 20,000 who went through the airport, 30,000, or whatever?

Mr. BRILL. We will give you that, but I will tell you it is not reflective of the program. What TSA asked us to do was take very specific—not a survey, but person by person, second by second metrics for the first 45 days or 6 weeks of the program.

So the average there is sort of halfway through from when we had nobody going through, because it was the first day of the program, to the 45th day.

Mr. THOMPSON. Well, would it be too much of a bother for you to update this—

Mr. BRILL. No, it is not a bother at all. We continue to do it. And we will give you more detail on the piece of paper you have in front of you, but also an update on that.

Mr. THOMPSON. That would also give us the passenger numbers, which we can obviously get, but in terms of what you are comparing it to?

Mr. BRILL. Right. One of the things we are doing, I should add, is we are engaged with various consulting firms that do airport modeling, so that we will know that, when we have 20,000 members in Orlando, or 40,000, and it is 8 o'clock in the morning on

Tuesday, how many lanes we need to have versus how many lanes the non–R.T. customers need to have.

We are doing an elaborate matrix of that. And, you know, we can give you some of that detail, too.

Mr. THOMPSON. One other question, Mr. Chairman.

Mr. Rotenberg, given what you have shared, the ease of acquiring certain information that probably should not be available, have you offered any suggestion, or can you offer us some suggestions as to, from a privacy standpoint, how we could fix this?

Mr. ROTENBERG. Well, certainly, sir. If the private sector is performing a public function, which is passenger screening, then I think those organizations should be subject to the same laws that federal agencies would be subject to, to protect privacy.

And the Federal Privacy Act is actually a very good law. We have said over the years that, as long as the agencies follow that law, that will do well to protect privacy in the United States.

Where we run into trouble is where government functions go to the private sector or where a government agency says that they want to exempt themselves from some of those obligations. But the framework is very good, and I would simply suggest to apply it here.

Mr. THOMPSON. Thank you, Mr. Chairman.

Mr. ROGERS. I thank the gentleman.

Mr. Rotenberg, I want to go back to your three goals that you described a little while ago, and I fully agree with the second one.

The third one I do not fully understand. I would like for you to revisit that and talk more about your concerns over an endgame. Flesh that out for me, if you would.

Mr. ROTENBERG. Well, sir, obviously our concern with this program, as with many of the post–9/11 security programs, is that they seem to develop a life of their own.

As I said during my statement, there is no disagreement about the need to protect the country and to identify terrorist threats. But, of course, a lot of times an agency obtains data and finds that it has other uses. And there is a tendency for data to chase applications.

Now, I am not surprised by Mr. Brill's proposal. If I was in his situation, I might very well be doing the same thing. He is developing a service that can identify, based on watch list data, who is safe to fly in the United States.

Office buildings in Washington would like to know who is safe to enter those buildings. Theme parks in the United States are making decisions about whether they need to know more about the families that go there.

But you can see very quickly where this is going to end up. And I could imagine a scenario not too many years out where a person applying for a job, trying to get into that office building in midtown Manhattan, does not happen to have one of Mr. Brill's cards.

Now, if I am an employer in that building and I am told by somebody that someone I am about to hire—for whatever reason, maybe he did not take the time, maybe he did not have the money, maybe he did not bother—could not clear that access procedure to get into my building, I am going to have some thoughts about whether to hire him.

And I see those risks all the way down the line, if this goes forward.

Mr. ROGERS. Mr. Brill, do you have a response to that?

Mr. BRILL. Yes, let me take a crack at that. I might not have made what I had in mind as clear as I should have. Or maybe I did.

[Laughter.]

Either it worked or it did not work.

I have this vision of something called the voluntary credentialing industry, but it does not mean that if you do not volunteer you do not get into an office building, or you do not get to watch a basketball game, or you do not get on the Staten Island ferry.

What it means is that, today, there are risks other than airplanes. Much of the work of this committee has been devoted to looking at those other risks.

There are ferry systems that are at risk. And yes, indoor sports arenas have risks. That is why they now have, you know, souped-up security operations.

But, today, those people have one choice—actually, two choices. They can search no one, because it is just too much trouble and you cannot have a bottleneck to go into a basketball game or get on a ferry, or they can search everyone.

If they had another choice, which was—we now know that 30, or 25, or 40 percent of the people coming through have this card because they got it at an airport, because there is such critical mass—and, by the way, in my written remarks, you will see that I favor giving this card for free to law enforcement officers, because they have already gone through the screening to have a card like this.

This card should be given at a deep discount to hospital workers, and construction workers, and people who have already given their fingerprints and already been screened.

So if a critical mass of 30, 40 percent suddenly shows up at a basketball game, and you know they are going to have this card, then you can make the decision, “Well, maybe we can search the other 60 percent, whereas today we do nothing.”

Risk management is about having a tool that says there is a better way than all or nothing. And that is the only simple—I do not propose that we set those rules.

I agree completely with Mr. Rotenberg, by the way. We should be regulated just the way the federal government is regulated by the Privacy Act. If CEOs of companies like ours violate these promises, there should be criminal penalties. We favor the strongest regulation.

We have held ourselves to that regulation, by the way, by making our promises part of our contract with our customers, so they can hire a class-action lawyer and sue us the day we violate any one of these things.

But the government should regulate us. That is true. He is completely right about that.

Mr. ROGERS. Excellent. Thank you very much. I appreciate it.

The chair now recognizes the gentleman from Washington for any questions he may have.

Mr. DICKS. Mr. Rotenberg, let's go back to the watch list. In your statement, you point out some difficulties with this watch list, in terms of being able to get off the list.

Tell us what your major concerns are.

Mr. ROTENBERG. Well, Congressman, simply stated, a person is placed on the watch list and they do not find a way to get off it. And they are pulled aside repeatedly.

As you said earlier, there is anecdotal information. We have pretty good documentary information from the TSA. There has to be a way to get off these lists. I do not think—

Mr. DICKS. And you are testifying that still today there really is not a way to get off the list?

Mr. ROTENBERG. That is correct, sir. That is my understanding.

Now, I know that the TSA has been trying to fix this problem, for obvious reasons. I mean, it is a real problem. And I think they need to fix it.

But we have not yet seen the procedure, the effective redress procedure that gets a person off a watch list. At best they seem, as was described earlier, either to receive a letter from the TSA—I am not sure how that would work—or some verification number to explain that the records have been referenced and the problem has been resolved.

But neither of these procedures, if they exist, are routinely used.

Mr. DICKS. You know, aren't there ways you could put in an address or some other thing so that the person could differentiate himself from the person who is one the list for a good reason?

Mr. ROTENBERG. Well, that may be the way to go. I mean, I think that TSA has to solve this problem, because they are the ones, in effect, that are enforcing the use of this data. Of course, it is shared across federal agencies. The TSA is not the only agency.

But they are the ones who probably have the most interaction with the American public, because people are kept off planes when these errors occur.

Mr. LUNGREN. [Presiding.] Would the gentleman yield on that?

Mr. DICKS. Yes, I yield.

Mr. LUNGREN. Part of the question we have had before is whether or not TSA would be allowed to query commercial information banks, databanks, that might be able to differentiate by way of address or some other mechanism, to show, for instance, when we had John Anderson, the former presidential candidate here, who happens to have been caught a couple of times on watch lists because evidently there is somebody else with the same name.

But then people have said that that raises its own privacy concerns. Would you believe we ought to go in the direction, which would not allow TSA to own that, but would allow them to query a number of different commercial databanks to see if, in fact, they can differentiate these people?

Mr. ROTENBERG. Well, I will just mention, Mr. Chairman, that the advisory committee of homeland security that works on privacy issues looked at this recently. I do not know if you have seen their report yet. But they actually recommended against the use of commercial data.

Mr. LUNGREN. No, but I was asking for your opinion.

Mr. ROTENBERG. Well, I agree with them. I think the report is useful, because it suggests that you will actually introduce more sources of error, believe it or not—I mean, it may sound good to get more data, but then you introduce more problems about how you reconcile information now held by a government agency and maybe held by a credit reporting agency.

Names are misspelled. Addresses are changing. It is not a simple problem to solve. I do not know the solution.

And I wanted to mention, also, Mr. Chairman, I spoke recently with John Anderson. He asked me to come and talk about this issue at his law school. He is still very concerned about it.

Mr. DICKS. Let's go back to this business model, Mr. Brill. Explain again how this is going to work.

You are going to have competition between companies at each airport. And then each airport is going to decide how to—

Mr. BRILL. I think that Administrator Hawley was—what he was alluding to, that there are several possibilities. I must tell you, I got to know Mr. Hawley very well when I was doing a book and I admire him greatly.

And I guess I would be candid to say, when I knew him, he was running the go-teams at TSA. And Justin Oberman was on one of those go-teams. And I wish they would do a go-team attitude with this thing instead of the way they have laid out this schedule.

I do not think this is that hard. The business model can be what the airport decides as its agenda or the airline, which controls a terminal, can make it.

For example, we are in discussions with one airport that we are very close to having an agreement with where we are signing with them a non-exclusive concession agreement. We are saying, "Let us in. Let us operate. And if you let someone else in to operate, that is okay, too. We will compete in that airport."

Now, other airports, such as Orlando, offered an exclusive, in effect, concession agreement, but that does not make it captive.

And it does not make it exclusive once there is interoperability, because Larry Zmuda over here from Unisys, if he has a program, and he will, he can set up shop in downtown Orlando, or at the convention center, or anywhere he wants, and sell his cards against our card in Orlando. And we will be competing.

So we have to compete on three bases, privacy—I think is the thing customers are most concerned about—price and customer service. And as long as you do everything you can to make this a hotly competitive playing field, including the possibility of competing business models, then this can spread very rapidly.

I do not think the government, or the airport authority, or anybody, even Congress, should attempt at this point to figure out an industry that is just being born. I think what Administrator Hawley was saying is, we want to watch this happen, and we want to allow for different business models.

Mr. DICKS. Is there an anti-trust concern about, if you have to make these cards interoperable? I think that is the right phrase.

Mr. BRILL. There would be definitely—

Mr. DICKS. Would there have to be—some kind of an anti-trust waiver? Because each company would have—you know, then you would have to share information about your card with the other person.

Mr. BRILL. No, and I am glad you mentioned that. The most important thing about interoperability has to be that, whoever manages it, whether it is AAAE Clearinghouse or anybody else, what they should manage is a unique—and I think Marc would agree with me—a unique identifier, not the names, and the customer information, or anything else, about that person.

And we had a meeting over at AAAE yesterday, and they said that.

Second, as long as the only thing that clearinghouse does is set the rules, the technical rules, for us to exchange, but does not tell me, or Larry Zmuda from Unisys, or anybody else, or an airport what they can charge, how they should market it, or anything else, as long as, you know, those rules of in an "orderly marketplace"—which is where anti-trust violators get into trouble when they start talking about orderly marketplaces—as long as they do not do any of that, then it is fine to have interoperability and have rules, just technical rules, that basically say, "My card has to work with his."

Now, he and I have already said our cards are going to work together. We could sit in a room and do that. Again, I am not sure why this has to be some big committee, as long as someone makes us—

Mr. DICKS. All you have to do is show the card?

Mr. BRILL. No.

Mr. DICKS. Or does it have to go in through a machine?

Mr. BRILL. You put the card into a kiosk, and then you put your thumb or your iris image, whichever you have chosen when you enroll to be your primary.

Now, we use the same kiosk maker—that we use, I think, Unisys uses. And this technology is no longer rocket science. This is off-the-shelf stuff. If it was rocket science, I would not be sitting here talking to you about it.

Mr. DICKS. All right.

Thank you, Mr. Chairman.

Mr. LUNGREN. Mr. DeFazio?

Mr. DEFAZIO. Thanks, Mr. Chairman.

Mr. Barclay, as I understand it, you are doing the airport work on a cost-based, nonprofit basis, is that correct?

Mr. BARCLAY. Yes, sir.

Mr. DEFAZIO. Okay. Would it be possible to extend a system so that we could have a cost-based, nonprofit model for a trusted traveler card?

Mr. BARCLAY. That is where the clearinghouse portion of the thing, that is exactly what we are proposing and have been told by our bosses to do.

Mr. DEFAZIO. Okay. So you are saying the services you provide, which would be to actually input the data for the person and get a clearance, yes or no, would be nonprofit, cost-based?

Mr. BARCLAY. But we would not be inputting the data under most of the models. What a clearinghouse does is, you have got 400-plus airports—

Mr. DEFAZIO. Right.

Mr. BARCLAY. —which all have to feed information in. They all do it a little bit differently, but it is got to comply with some basic standards. And then you have got to make sure it goes into government in the right way the government wants to see it all.

Mr. DEFAZIO. Right, well, that is where you come in.

Mr. BARCLAY. That hub part is the only part that we wind up doing.

Mr. DEFAZIO. Right.

Mr. BARCLAY. The collection of the data itself—

Mr. DEFAZIO. But you have done this at individual airports around the country?

Mr. BARCLAY. Yes. We currently do that for airport employees.

Mr. DEFAZIO. Right. So you could have a system where, perhaps, we cut out the middleman, people could come to the airport, they could fill out a form, input their data, and we would not have a private vendor messing with their privacy information at all?

The government would say yes or no to the vendor that they could have a card. I mean, that is the way, for instance, the purchase of a firearm works today. The firearms dealer does not get your record. They do not get anything other than your basic identification. They get a yes or a no.

Couldn't we have a system like that, so we do not have to worry about the private vendors?

I mean, I have heard from Mr. Brill. Except two words come to mind: ChoicePoint. There are a few other words out there about massive privacy losses, where individuals have no recourse. It is like, "Oh, sorry, your data has been compromised. Your identity has been stolen, but"—

Mr. BRILL. Well, Congressman, you still have the—

Mr. DEFAZIO. No, I did not ask him. Mr. Brill, Mr. Brill, I will get to you in a moment. I am just asking Mr. Barclay.

Mr. BARCLAY. Sir, it is technically possible to do it that way—

Mr. DEFAZIO. Okay.

Mr. BARCLAY. —but it has not been the selected model that we have been—

Mr. DEFAZIO. Okay. Well, and Mr. Brill, if you were closely following the Republican Congress, they are dramatically restricting class-action lawsuits. You were talking about class-action lawsuits against you or others who have violated their contracts, but we are pretty quickly doing away with that option for consumers.

But let me go to your comments, Mr. Brill. You said that I did not characterize it properly. Let's go through this step by step.

You competed to get a contract at Orlando, correct?

Mr. BRILL. Correct.

Mr. DEFAZIO. Okay. Now, were you the low cost, in terms of the charge to the consumer?

Mr. BRILL. It turns out we were, yes.

Mr. DEFAZIO. Okay. Were you the largest cut to the airport?

Mr. BRILL. Excuse me?

Mr. DEFAZIO. Did you give the largest percentage to the airport of the proposals?

Mr. BRILL. Yes, we did.

Mr. DEFAZIO. Okay. All right, so we have the lowest cost, but the largest to—now—

Mr. BRILL. That shows pretty good management.

Mr. DEFAZIO. —what is an individual's choice when they go to Orlando? Can I call up a competitor and get another card, or do I have to buy your card, if I do not want to stand in the 31-minute line?

Mr. BRILL. Well, one of the reasons I am here is to get individuals that choice by having an interoperable—

Mr. DEFAZIO. Right. That would be good. But it does not exist today. And I want to make certain that it does.

Now, I guess I would wonder why this has to be airport-based at all. And I would put that to any member of the committee. If we are truly going to have, as I put to Mr. Hawley, people out there offering competitive cards, why should the airports be involved in that at all?

Mr. BRILL. Well, I can give you what we have been told by TSA, which is their view that, for them to operate, and authorize, and regulate a program, they have to do it in contract with, or agreement with, a regulated entity, one of which can be an airport, the other of which can be an airline.

And I think the airlines are likely to get into this, too. But could they do it with, you know, a retail operation not at the airport? I guess. But they do not think they can.

Mr. DEFAZIO. The kiosks are becoming fairly standard technology. If we just adopted a standard for kiosks, and anybody could sell a card that would work in that kiosk, who has been vetted, confirmed, and not be al-Qa'ida or somebody else, you know, to be a proper business entity, now that would give true competition.

I remain extremely concerned—and as I said to you in the office and here—that, if you got a lock through the airports, who are desperate for revenue, or you got a lock through the airlines, who are desperate for revenue, that we are going to find big add-ons for them and that consumers are not going to have that many options.

Now, if every airport is doing it then, yes, maybe you will have some competition and some of them will undercut other public entities and try and do that, but I really do not believe the airports should be getting a cut. I just do not believe it, and I do not see why that should be, that an airport would get a cut.

I was the Democratic sponsor of reinstating passenger facility charges. They had been hugely abused by airports, public airports, across America, where they were running the airports and their local government on charging people at the airports. They were done away with for almost 20 years.

I can see the same thing happening here. I mean, I have already had airports come in. They want to stretch PFCs. They want to stretch the definitions.

They are desperate for revenues. "Oh, here is a new profit center. We are going to get a 25-percent cut on every card at our airport."

I have tremendous concerns about industries and/or entities under pressure that get a cut. So I would suggest that a proper business model would be the kiosks are installed, you know, how they are installed, the airport has to be involved in that.

But the card itself could be marketed by anybody in that interoperability. And then you would have true competition. But absent that, you are not going to have true competition.

Mr. BRILL. May I just respond to that for half a second?

Mr. DEFAZIO. Sure.

Mr. BRILL. I will leave to—the issue of whether airports should or should not charge a fee. We were presenting—

Mr. DEFAZIO. Well, he did not take much of a position on that.

Mr. BRILL. Well, I mean, if I were paying less of a fee at an airport, obviously, I would like that better. And we would have a lower cost to the consumer.

But the issue of simply having a kiosk at a grocery store or a 7–11 for which you could—I probably have not been—

Mr. DEFAZIO. No. We are talking about kiosks at the airports that you plug the card into—

Mr. BRILL. Well, but it is not that easy.

Mr. DEFAZIO. —like the one that is sitting idle at National today, for instance.

Mr. BRILL. We employ 54 people at the Orlando Airport to do that enrollment. You have to take people's prints. You receive their documents. You have to make sure their identity documents are authentic. We put those documents through machines. It is not an automatic process.

Mr. DEFAZIO. Right. But you do not have to do that at an airport. I mean, you could be MasterCard and doing it all around America. You do not have to be at an airport to do it.

Mr. BRILL. We have to screen our employees, and we have to train them, and we have to do it. I am not suggesting that the airports or any venue should have a monopoly on sales of this. I am simply suggesting that it is a little more complicated than simply—

Mr. DEFAZIO. I am not saying it is simple.

Mr. BRILL. —than going to a soda machine and buying a can of soda.

Mr. DEFAZIO. It is becoming a very complicated process, by virtue of the fact that we have a government that is obsessed with privatization and, instead of having a standardized technology chosen in a competitive bidding process with a vendor nationwide and installing that nationwide, and having the people who use it pay for it, they are obsessed with some sort of lame semi-competitive model that might or might not involve airports, might or might not involve airlines, might or might not involve other vendors.

They do not really know. "That might be an interesting business model. Gee, we do not know. We want to see what they propose." And somehow we are going to get great security, a low price, and integrity out of this system?

Because we want to go all the way around the barn instead of saying, "This is pretty simple. The government will ask for vendors. The vendors will compete. Somebody will win with a low bid, and they will install the equipment in the airports nationwide. And then we will defray the costs."

Instead, you know, that is—

Mr. BRILL. Well, sir, you mentioned ChoicePoint. Who does a customer who has signed up in a government program—now, I might remind you that the Registered Traveler pilot projects involve 10,000 people and I think they cost $13 million.

Mr. DEFAZIO. I am not saying that this administration is efficient, effective, or runs government well, or runs it like a business.

And I am not defending their miserable record in transportation security or any place else. So they are not a good model.

Mr. BRILL. I was not actually assuming you were.

Mr. DEFAZIO. And I understand. That is fine. But what I am saying is the government could, by competitive contracts, have all that work done and have it standardized nationwide.

Mr. BRILL. But the question I was going to raise is, if I violate one of our customer's privacy—we have very specific standards—they can sue me. They can cancel their membership.

They can get our customer service people on the phone 24 hours day. They can usually, in fact, get me on the phone, or by e-mail, because I have a profit incentive. These people are paying us $79 a year, and I am obsessed with getting them to renew their subscription.

I say, with all due respect, that the way to make this program work is to make it competitive and not have a government contractor be given $4 billion, or $5 billion, or $10 billion, or if you extrapolate from the pilot project, $35 billion to do a program where you will not be able to get anyone on the phone.

You will have no redress if your privacy is violated, except, I guess, to write to your congressman. And you will have no lawsuit. You will have nothing. And I do not think the program would work as well.

Mr. DEFAZIO. Well, that is one view of the world. But this mishmash that they are proposing, which—you know, it is just not clear to me that we are going to have an interoperable technology. We are going to have multiplicity of vendors, which may or may not have to get an airport to sponsor them to become a vendor, may or may not have to get a desperate, bankrupt airline to sponsor them to become a vendor.

And then somehow this is going to become a program with integrity, and it is going to be universal, and it is not going to discriminate against small airports, as opposed to large airports, with its competition, and all the other problems we have had with competition in this industry.

So I know you have faith in what you are doing. I am sure you provide a good product. At this point, it is small and manageable. But I have concerns about the indifference of the administration, which is, "Well, they will come in with stuff, and we will kind of figure out a process, and we will choose something."

They are not even saying—you know, they do not have any vision at all about how this is going to work at the moment. They are not even saying it is going to be airport-based.

Thank you, Mr. Chairman.

Mr. LUNGREN. And I just want to make it clear, Mr. DeFazio, I would never accuse you of defending the administration.

[Laughter.]

I would like to ask some of my questions that I missed before.

Mr. Zmuda, you have been sitting there quietly with no one asking you a question. I feel compelled to give you a chance.

And my question would be something that would be directed at both you and Mr. Brill, and that is, what is the incentive, what is the possible incentive for you in the private sector to invest your resources into the screening technology at the airports?

You do not actually do the screening. You are prior to the screening. You are giving them people that they can identify in a certain way. Or would you have any incentive to do that?

Mr. ZMUDA. No, our incentive is not to take over the job of TSA to do the screening. Our job is to support and provide benefits to the traveling public, to provide them an expedited process.

By providing the security systems that TSA currently employs and staffs, then you are getting into decisions on security. And those are things that the private sector should not make a decision on. So, from my perspective, there is no incentives for me to get into TSA's job.

Mr. LUNGREN. Mr. Brill had suggested there would be an incentive to make capital expenditures to allow the use of the newest technology in those lines that are dedicated to the Registered Traveler. Would you accept that as part of your business model, or would you allow him to do that as your competitor and not worry about it?

Mr. ZMUDA. No, I think, in terms of testing out the latest technology, whether it is RFID capability or facial recognition, as that new technology can be introduced into the marketplace, it is something that we definitely want to invest in, because, like Mr. Brill stated, the goal is to provide the best product to the customer, where they are going to want to sign up for this program and also receive a benefit, all in the same time ensuring that the security of not only the airlines but the airport is remaining intact.

And that is why there has to be that separation between services that the private sector provides upfront, and it remains separate from what the TSA does in the security checkpoint process.

Mr. LUNGREN. Let me ask Mr. Barclay, and Mr. Brill, and Mr. Zmuda this question. That is, some would say that al-Qa'ida and their affiliates, or even the wannabes, are very good to adjust to whatever we might do. Wouldn't this give them a better opportunity?

Here we are giving people a free pass. They pay $75 or $100. And one of the attributes of the program, as you, Mr. Brill, have talked about, and you, Mr. Zmuda, have talked about, and, Mr. Barclay, being with the airports, you folks have suggested you do not go through quite the same screening that everybody else does.

You would not have to take your coat off. You would not have to take your shoes off. You would not have to have your P.C. opened up and looked at. Wouldn't that create a vulnerability?

Mr. ZMUDA. Well, one thing that you do have, it is part of a layered approach. Because the people that enter this program first have to provide, you know, government documentation and a photo I.D. that can be checked to make sure that is not a forged document.

Then the next process is providing fingerprint and iris, or whatever the biometric that is determined. And then, from that point, the background check.

And then, even after those layered approaches, you still have to go through some security checkpoint that the TSA provides. So that layered approach to security is one way to counter what you were just looking at.

Mr. LUNGREN. Mr. Brill?

Mr. BRILL. We have stated explicitly that we want to and, in fact, we are already talking to vendors of equipment. And while that is something that will help us move people through faster, it also adds some security.

But, you know, the basic point is that every security system has holes. And the difference is the trade-off between what you get by taking a risk management approach and what you get by just making people selectees because they had their flight cancelled and they have to fly through, you know, Phoenix instead of Dallas.

Are we safer as a country through that approach versus this approach? But I do think that there are lots of ways to plug those holes.

One of the things that Mr. Hawley mentioned is, in part, the randomization of searches even for members. And I will tell you that I have never heard a security expert say anything other than the fact that, no matter what system you are using, you do need to have some element of randomness to it. The question is, how often and how widespread that is.

Mr. LUNGREN. Mr. Barclay?

Mr. BARCLAY. Yes, I think the argument that this could be gamed by al-Qa'ida is an argument you have to use when you look at the fact that we trust background checks to let federal air marshals on airplanes with loaded guns. We let law enforcement on airplanes with loaded guns.

We use the notion of background checks of people to trust that they are reliable in the system and not threats to the system. And we try to get those, that background check process, as tight and as good as you possibly can.

But it is not just true of registered travelers, if you have a problem with that. It is true of a lot of people we currently trust in the system.

So, as Steve said, there is no perfect system. But you can run a very tight system. And, overall, you can get a higher level of security, we believe.

Mr. ROTENBERG. Mr. Chairman?

Mr. LUNGREN. Yes, Mr. Rotenberg.

Mr. ROTENBERG. If I could just have a word on this. Actually, I had the opportunity to address this issue before the 9/11 Commission.

And the point that I made then is that I think it is very important, particularly with aviation security, to keep the focus on devices and instrumentalities that pose the threat, as opposed to the individuals.

And I can tell you that the threat scenario for the Registered Traveler program is not generally very well understood. I do not think it is the case that we have to be concerned that someone in deep cover is going to be authorized under Registered Traveler to board a plane.

I think we have to be concerned about that someone else is going to exploit a person's Registered Traveler status to get a device, an explosive, onto a plane that causes the harm.

And I am sad, actually, that Mr. DeFazio is not here, because I think he made a very good point at the opening of the hearing, with explosives being a primary threat to aviation security. Anything that might diminish our ability to detect the presence of explosives on an airline passenger, whether or not that airline passenger is aware of the presence of the explosive, actually poses a threat to our nation's security.

So I hope nothing about this program leads to a reduction in efforts to detect those devices or weapons that might threaten passenger safety.

Mr. LUNGREN. Thank you.

Do you have any more questions?

Mr. THOMPSON. Thank you, Mr. Chairman.

I guess the comment is, for all four of your gentlemen, is that we have been toying with Registered Traveler program for about 3 years now. There appears to be significant support for it in Congress, as well as the traveling public.

Why do you think the program is slow getting off the ground?

Mr. Barclay?

Mr. BARCLAY. I will start, Congressman. It was a privilege of mine to be appointed by Secretary Mineta right after 9/11 to one of the rapid response teams for airports, together with several airline CEOs and some other security experts.

And the very first recommendation, back right after 9/11, was we need a Registered Traveler, at that time a trusted traveler, program in order to make the haystack smaller, as everyone keeps talking about.

And it was understandable, when TSA started, they had a whole lot of priorities on their plate, including standing up an agency that was extraordinarily large.

And it seems like this has always been a issue. Every time it gets up to the top of somebody's pile who is the head of TSA to make a decision on—Kip Hawley, who is terrific, is their fourth leader of TSA. And it has been one of those programs that keeps seeming to run up and down the pile, because of other priorities that have been perceived.

So, hopefully, with the time line that Assistant Secretary Hawley set out today, we are really on the right path.

Mr. BRILL. In part, a lot of this is complicated stuff. And I do not want to minimize it. I do think there was a lot of debate early on, first of all, over whether a program like this was necessary.

Because, if you will recall, the original CAPPS II, I guess it was going to be, or CAPPS I, whatever, you know, was going to work so well that it would classify everybody. So why would you need it, I think is what some people in Secretary Ridge's office thought.

And these are significant policy issues. And then there are the questions of what the business model would be. But having said all that, I think we are now at a point—I mean, we were asked to submit data from Orlando.

Orlando was ostensibly a pilot project. We submitted the data, I think, 5 days before the deadline and the day after we collected it. They have had it since September 26th. They can evaluate it. It is pretty clear.

I think Administrator Hawley made clear that they have made their basic value judgments and they are moving forward. I have the same question, I think, you or one your colleagues asked, which is, “I do not understand what in a voluntary program they would need a year’s worth of rulemaking on the criminal records check.”

I do not understand why they have to wait until April to some of the things they said they were going to take until April to do. But I am just a naturally aggressive and frustrated person, because I want to get this thing done, and I have been working on it for 2 years, so I am not the person who has very good perspective on this.

Mr. ZMUDA. I think there is basically three areas that the TSA has been wrestling with. I mean, one of the things that came out of the pilots was testing out different technology.

At one airport, we did not even use smart cards. Other airports, we used a different type of card. And then, in a third, we used an actual smart card with the biometric and biographical data on there.

So evaluating all the technology that was deployed in the pilots was one thing that TSA needed to take into consideration. Transferring this from a wholly owned public model, which the pilots were, and transitioning it to a public-private partnership took additional time.

And airlines and airports, as well as the traveling public, are looking at policy decisions to alleviate some of the things that are needed, such as, you know, taking out the laptops and so forth.

I think all of those TSA has been able to make decisions on. And I am hopeful that, you know, with the rest of the people at this panel, that, given all this information and decisions, we can roll out.

If it is earlier than April, I think I would be ecstatic, as well. But hopefully they have all the information that is necessary.

Mr. ROTENBERG. I think this is, as the computer scientist would say, a hard problem. It is not so difficult to make a device that can detect whether someone is carrying a gun onto a plane or to make that device very sophisticated, if the gun is made of other materials.

But to create a device that relies on personal data that can determine what someone’s is intent is when they board the plane is much, much more difficult. And even though it might be tempting to say, if someone is properly cleared, we can put them on the plane with assurance that nothing bad will happen, we know that in practice it is not that simple.

And I do not see a simple solution to this, which is why I do believe you should continue to focus on the detection of devices that pose a threat to aviation security.

Mr. LUNGREN. Thank you, Mr. Thompson.

And I thank the witnesses for their valuable testimony and the members for their questions. The members of the committee, as you may have heard before, may have additional questions for you in writing. And, if they do, we would ask that you would respond to them in writing.

The hearing record will be held open for 10 days.

And thank you, once again.

Without objection, the committee stands adjourned.

[Whereupon, at 2:31 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS AND RESPONSES FOR THE RECORD

QUESTIONS FROM HON. DANIEL E. LUNGREN FOR CHARLES BARCLAY RESPONSES

1. The statement of principles you have circulated to members of your Registered Traveler Interoperability Consortium seem to imply that those airports that do not join the consortium and abide by the rules it established—including "business rules" and rules related to how RT programs are marketed and advertised—will not be able to have interoperable registered traveler programs. Yet in your testimony you state that membership in the consortium is voluntary. **Can you explain?**

Answer: The Registered Traveler Interoperability Consortium was formed by a group of airports to establish common business rules and technical standards to create a permanent, *interoperable* and vendor-neutral Registered Traveler (RT) Program that will bring passenger screening consistency and improved security procedures to air travelers in the United States. From the very beginning, the RTIC has strived to be as open and inclusive as possible, inviting all airports, airlines, and interested vendors to the table to participate in the establishment of standards necessary to ensure that the program is nationwide and interoperable. Membership in the RTIC has always been, and will continue to be, voluntary. We are pleased to report that more than 60 airports of all sizes from all areas of the country are involved in the RTIC effort along with virtually all vendors with an interest in the RT program.

While the RTIC does envision playing a key role in the establishment of those standards and looks forward to working closely with TSA on their ultimate adoption and implementation, we believe that non-participating airports maintain the freedom to make decisions locally about what vendors and service providers offer the best alternative at their facility consistent with the standards ultimately approved by TSA. With common standards and an open-architecture, we believe that each airport will have the autonomy necessary to design local solutions to unique local situations while being part of an interoperable RT program.

2. **The same statement of principles says that members of the consortium will vet and certify service providers. Yet, Mr. Hawley's testimony stated that TSA was going to certify service providers. Can you explain? And are there airports who are members of this consortium willing to assume the liability attendant with such certification?**

Answer: As Director Hawley pointed out, TSA will have responsibility for the regulatory function of certifying vendors that participate in the program. The RTIC's role with regard to "certification" is merely to assist TSA in ensuring that participating vendors are meeting the standards established by TSA in an operational context—that is to say that they are conducting business on a day-to-day basis in a manner that is consistent with the security, operational, and technical standards established by TSA or airport operators.

3. **Do you intend for the clearinghouse to keep any central repository of names and personally identifying biographic and biometric information?** We understand that the service providers, the airlines, and privacy groups want to keep this information decentralized, that is, in the service providers' own secure date warehouses, and simply transmit to the clearinghouse a unique identifier for each member, in order to assure privacy and security and prevent there from being one central source of such information. **Do you agree that the clearinghouse should assume this limited role?**

Answer: There is not yet unanimity regarding the utilization of a centralized biographic and biometric database, and at this point no final decisions have been made by TSA, airports, or vendors interested in participating in the Registered Traveler program with regard to the specific utilization of the Transportation Security Clearinghouse. For our part, we are committed to meeting the requirements for the clearinghouse—whatever they may eventually be in order to enhance the efficiency and security of the program. We believe that the ongoing RTIC process and TSA's public comment process will ensure that the concerns of service providers, the airlines, privacy groups and others in this area are appropriately addressed, and the clearinghouse is committed to operating in compliance with whatever standards are established in this area.

4. **What exactly will the clearinghouse charge?** Your testimony referred to $7 to $25.00, but those are amounts charged for actual vetting against data bases. Here TSA has made it clear that it will provide a charge for vetting and the AAAE would simply be providing an exchange service for names or unique identifiers, a service that technology experts tell us should cost pennies per member per year. **Please tell us what you would charge, and how you intend to assure that this is a market-driven charge.**

Answer: Currently, the charge for processing fingerprint-based criminal history background checks for airport and airline employees is $29—$7 of which goes to the Transportation Security Clearinghouse for a host of functions including technical and administrative work and other duties assigned by TSA. The $29 figure compares with the roughly $100 that is currently being charged by a different entity to process criminal history background checks for HAZMAT truckers.

Since the specific functions for the Transportation Security Clearinghouse have yet to be defined as highlighted in the previous question, it is impossible to say what the TSC will eventually charge for services that TSA, airports, and vendors participating in the program may ultimately request. It is important to highlight for the Committee again, however, that the TSC is owned by our airport members and that those members are and will remain important TSC customers. The mandate that we have from our membership—the TSC owners—and from our partners involved with the RTIC is to be transparent and cost-based. We will continue to meet that mandate as we have over the past four years with the successful processing of more than 1.9 million criminal history record checks for airline and airport employees.

Again, I would remind the Committee of the successes of the TSC to this point:

- The TSC process has reduced the time it takes for airports to get fingerprint results from often more than 50 days, pre-September 11 when submitting to OPM, to an average of four hours, with many reports completed in around 40 minutes. This reduction in time has enabled airports to put their employees on the job where they are needed, without the need to pull another valuable employee from their duties to serve as an escort. The TSC has saved the industry hundreds of millions of dollars in productivity gains and employee retention as a result of reduced fingerprint check processing times.
- Because of innovative in-house technical work, the TSC performs "real-time" processing to transmit fingerprints to the federal system in an average of 16 minutes. The TSC's "real-time" processing dramatically increased the efficiency and timeliness of the airport fingerprint submission process.
- Centralization of the fingerprint tracking process allows for accurate fingerprint submission status at any point in the background check process virtually eliminating "lost fingerprints" within the federal system. Ensuring that airport employees can return to work and not have to be called back for repeated fingerprinting due to missing fingerprints this centralized process has saved airports thousands of wasted employee work hours over the last three years.
- Because of AAAE's ability to do the technical and administration work "in-house" and subsidize labor and other costs for the formation of the clearinghouse, the resulting cost savings allowed TSA to lower fingerprint processing prices from $31 to $29 (for electronic submissions), saving the industry over $3 million dollars.
- FBI indicates that the submissions of the aviation community done through the TSC had one of the best error rates in the U.S. (2%) and that this reduced error rate was directly related to the quality checks and error corrections performed by the TSC. The current federal average error rate is 8%. Since the TSC began operations, the error rate has continued to decline, with a significant drop when the TSC brought its "in-house" developed software package online. This equates to approximately 32,000 aviation workers that did not have to go through the time consuming process of reprinting due to errors created at the airports' print office with a cost savings of $2.5 million dollars to the industry.

The TSC is owned and controlled by its key customers—public airports—and has a four-year track record of modest, cost-based charges. We will continue this operating model in the future because it is built into the TSC's structure.

HON. DANIEL E. LUNGREN QUESTIONS FOR HON. KIP HAWLEY RESPONSES

1. The statement of principles circulated by the American Association of Airport Executives to members of the Registered Traveler Interoperability Consortium (RTIC) seems to imply that those airports that do not join the consortium and abide by the rules it establishes—including "business rules" and rules related to how RT programs are marketed and advertised—will not be able to have interoperable registered traveler programs.

Is that the way you view AAAE's role? Please explain in detail how TSA will utilize the Transportation Security Clearinghouse for the Registered Traveler program.

Response: The Transportation Security Administration (TSA) expects to utilize the Transportation Security Clearinghouse (TSC) as a central data management system for the Registered Traveler (RT) Program per a Congressional mandate included in the FY 2006 Department of Homeland Security Appropriations Act. In this role, the TSC will collect biographic and biometric data from all participating enrollment providers. It will then aggregate and format the data to government specifications, and pass the data through to the Federal Government to conduct security threat assessments. TSA will ensure that all information collected and stored is technologically interoperable with other Homeland Security and Justice criminal and watchlist databases and properly handled to meet privacy and security requirements. The clearinghouse will also maintain a database of unique identifiers matched to security assessment results that will be distributed to all participating airports to verify the status of passengers at the security checkpoints.

In December 2005, TSA issued a Request for Information (RFI) seeking input from industry stakeholders regarding the business and interoperability rules that will govern the RT program. The precise role of the TSC regarding these rules and its relationship with other stakeholders will be considered as part of this effort. Comments are due to TSA no later than January 20, 2006.

2. **Does TSA support a level playing field for all service providers, regardless of whether they are members of the RTIC? If so, please explain how TSA will ensure this occurs?**

Response: The Transportation Security Administration (TSA) strongly supports a level playing field for all service providers, regardless of their affiliation with the Registered Traveler Interoperability Consortium (RTIC). The RTIC is a private entity, and TSA interacts with them on the same basis that the Agency interacts with other industry stakeholders. This principle of equal treatment is integrated into the RT development process as exemplified by the Request for Information (RFI) and TSA's having held an Industry Day that was open to the entire public. Through these means, TSA is broadly soliciting recommendations from all stakeholders regarding the RT business and technical models.

3. **The same statement of principles says that members of the consortium will vet and certify service providers. Yet your testimony stated that TSA was going to certify service providers. Can you explain?**

Response: The Transportation Security Administration (TSA) expects to procure an independent contractor to qualify all participating vendors. This contractor will use TSA guidelines and criteria to qualify vendors independent from the Registered Traveler Interoperability Consortium.

4. **The AAAE has convened a committee of service providers who, it says, are going to suggest business models for the RTIC (airports) to ratify. Your testimony stated that TSA was going to get input directly from the industry and makes its own decisions about the business rules, including the rules for interoperability. Can you clarify?**

Response: The Transportation Security Administration (TSA) will make all final decisions on the business model. Through the Request for Information, TSA has solicited input from the entire industry. The RTIC is simply one industry group that TSA hopes will provide input. The RTIC suggestions will be considered along with the input from other industry stakeholders.

5. It is my understanding that AAAE, through its RTIC, will present to TSA one agreed to business model for the RT program. **Did TSA request this approach or would TSA like to see multiple business models submitted?**

Response: Through the Request for Information, the Transportation Security Administration (TSA) has solicited various stakeholders to submit whichever business models they deem appropriate for TSA's consideration. TSA expects to review various business models in developing the RT business rules.

6. **Do you intend for the clearinghouse to keep any central repository of names and personally identifying biographic and biometric information?** We understand that the service providers, the airlines, and privacy groups want to keep this information decentralized, that is, in the service providers' own secure data warehouses, and simply transmit to the clearinghouse a unique identifier for each member, in order to assure privacy and security and prevent there from being one central source of such information. **Do you agree that the clearinghouse should assume this limited role?**

Response: The types of information to be kept by the Transportation Security Clearinghouse (TSC) will be determined in the final business model. The TSC will store a security threat assessment decision with a unique identifier for pass through to all verification providers in order to make eligibility determinations at the checkpoint kiosks on all participants in the program. Also, TSA will ensure that all information collected and stored is technologically interoperable with other Homeland Security and Justice criminal and watchlist databases and properly handled to meet privacy and security requirements. Any additional responsibilities will be defined in the business model to be published in the Federal Register and will be subject to a period of public comment.

7. **What exactly do you anticipate the clearinghouse will charge? Mr. Barclay's testimony referred to $7 to $25.00, but those are amounts charged for actual vetting against data bases. Here TSA has made it clear that it will provide and charge for the vetting and the AAAE would simply be providing an exchange service for names or unique identifiers, a service that technology experts tell us should cost pennies per member per year. Please tell us what will be the charge, and how TSA intends to assure that this is a market-driven charge? We assume that airlines that operate their own terminals will be able to create RT programs. The AAAE consortium does not seem to account for that possibility. Can you clarify?**

Response: The fee charged by the Transportation Security Clearinghouse (TSC) will be determined based on its role as defined in the final Registered Traveler business model. The Transportation Security Administration (TSA) will have a contractual agreement with the TSC making its cost structure subject to review.

TSA expects that TSA and not TSC will conduct the initial and recurring Security Threat Assessment.

Similarly, the final Registered Traveler business model will govern the role of air carriers in the program.

○