

**MANAGING RISK AND INCREASING EFFICIENCY:
AN EXAMINATION OF THE IMPLEMENTATION
OF THE REGISTERED TRAVELER PROGRAM**

HEARING
BEFORE THE
**SUBCOMMITTEE ON TRANSPORTATION
SECURITY AND INFRASTRUCTURE
PROTECTION**
OF THE
COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JULY 31, 2007

Serial No. 110-64

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

48-959 PDF

WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,	PETER T. KING, New York
EDWARD J. MARKEY, Massachusetts	LAMAR SMITH, Texas
NORMAN D. DICKS, Washington	CHRISTOPHER SHAYS, Connecticut
JANE HARMAN, California	MARK E. SOUDER, Indiana
PETER A. DeFAZIO, Oregon	TOM DAVIS, Virginia
NITA M. LOWEY, New York	DANIEL E. LUNGREN, California
ELEANOR HOLMES NORTON, District of Columbia	MIKE ROGERS, Alabama
ZOE LOFGREN, California	BOBBY JINDAL, Louisiana
SHEILA JACKSON LEE, Texas	DAVID G. REICHERT, Washington
DONNA M. CHRISTENSEN, U.S. Virgin Islands	MICHAEL T. McCAUL, Texas
BOB ETHERIDGE, North Carolina	CHARLES W. DENT, Pennsylvania
JAMES R. LANGEVIN, Rhode Island	GINNY BROWN-WAITE, Florida
HENRY CUELLAR, Texas	MARSHA BLACKBURN, Tennessee
CHRISTOPHER P. CARNEY, Pennsylvania	GUS M. BILIRAKIS, Florida
YVETTE D. CLARKE, New York	DAVID DAVIS, Tennessee
AL GREEN, Texas	
ED PERLMUTTER, Colorado	
VACANCY	

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*

ROSALINE COHEN, *Chief Counsel*

MICHAEL TWINCHEK, *Chief Clerk*

ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

EDWARD J. MARKEY, Massachusetts	DANIEL E. LUNGREN, California
PETER A. DeFAZIO, Oregon	GINNY BROWN-WAITE, Florida
ELEANOR HOLMES NORTON, District of Columbia	MARSHA BLACKBURN, Tennessee
YVETTE D. CLARKE, New York	GUS M. BILIRAKIS, Florida
ED PERLMUTTER, Colorado	PETER T. KING, New York (<i>Ex Officio</i>)
BENNIE G. THOMPSON, Mississippi (<i>Ex Officio</i>)	

MATHEW WASHINGTON, *Director*

ERIN DASTE, *Counsel*

NATALIE NIXON, *Deputy Chief Clerk*

COLEY O'BRIEN, *Minority Senior Counsel*

(II)

CONTENTS

	Page
STATEMENTS	
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas, and Chairwoman, Subcommittee on Transportation Security and Infrastructure Protection	1
The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, Ranking Member, Subcommittee on Transportation Security and Infrastructure Protection	3
The Honorable Paul C. Broun, a Representative in Congress from the State of Georgia	17
The Honorable Zoe Lofgren, a Representative in Congress from the State of California	18
The Honorable Eleanor Holmes Norton, a Delegate in Congress from the District of Columbia	15
WITNESSES	
PANEL I	
The Honorable Kip Hawley, Assistant Secretary Transportation Security Administration, U.S. Department of Homeland Security:	
Oral Statement	5
Prepared Statement	6
PANEL II	
Mr. Steven Brill, Chairman and Chief Executive Officer, CLEAR/Verified Identity Pass, Inc.:	
Oral Statement	23
Prepared Statement	24
Mr. Tom Conaway, Managing Partner, Homeland Security, Unisys Corporation:	
Oral Statement	21
Prepared Statement	22
Mr. Bill Connors, Executive Director, National Business Travel Association:	
Oral Statement	32
Prepared Statement	33

**MANAGING RISK AND INCREASING
EFFICIENCY: AN EXAMINATION OF
THE IMPLEMENTATION OF THE
REGISTERED TRAVELER PROGRAM**

Tuesday, July 31, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY
AND INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 1:45 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [chairwoman of the subcommittee] Presiding.

Present: Representatives Jackson Lee, Norton, Perlmutter, Lungren, Bilirakis and Broun.

Also Present: Representative Lofgren.

Ms. JACKSON LEE. Thank you for your patience.

Good afternoon. The subcommittee will come to order. The subcommittee is meeting today to receive testimony on the Transportation Security Administration's partnership with the private sector administering the Registered Traveler Program. However, before I begin, I ask for unanimous consent that Ms. Lofgren, a member of the full committee, may sit and question the panel during today's hearings.

Without objection.

Let me also acknowledge the presence again of Ms. Lofgren—welcome—a member of the full committee; Mr. Perlmutter, a member of the subcommittee; Ms. Holmes Norton, a member of the subcommittee who is present here today; and the ranking member, Mr. Lungren; Mr. Bilirakis, a member of the subcommittee; and we are very, very pleased to have, I would like to say, Dr. Paul Broun, who is a member of the subcommittee, a newly minted Member from Georgia.

And let me make sure that I have the pronunciation correct. It is Dr. Broun, Congressman Broun?

Mr. BROUN. Correct.

Ms. JACKSON LEE. We welcome you to the subcommittee, and I think that you will find that you are at the cutting edge of helping to secure America. We welcome you greatly.

Let me welcome our Administrator, the Transportation Security Administrator, Kip Hawley.

I will now yield myself the appropriate amount of time to begin my opening statement. I think, most timely for this particular

hearing—I want to thank the staff for their work, because we have been facing a number of added concerns over the summer travel season.

This is not a hearing on whether your plane was late coming to Washington today, but it is recognizing that we have challenges in the season, particularly as we have publicly read the National Intelligence Estimate which—I know that there is an enormous amount of chatter and concern about the actions of those engaged in that chatter.

We also know that we have faced, as I indicated in the hearing last week, a rather unusual set of circumstances in the Phoenix, Arizona, airport that was made public last week; and I made the point very clearly that that will have to cease and desist. And those were the actions shown by video of the airport being, in essence, uncovered by Transportation Security Administration personnel for a period of time, and that the entering and leaving was subjected to very minimal scrutiny and screening.

I do want to acknowledge that the Administrator and myself have had, I think, some in-depth conversations on this matter; we are working on the matter. There is still an opportunity for us to hold hearings on this issue, but it is all in the larger picture of, how do we thoroughly secure the Nation's airports and the Nation's transportation system.

With that, I would like to begin to take this opportunity to thank you all for joining us this afternoon so that we can begin our exploration of the Registered Traveler Program.

In the wake of September 11th, aviation security was made a Federal responsibility. And I think everyone here today would agree that aviation security has improved substantially. Protecting the Nation, ensuring aviation security has required a layered approach. Now, this layered approach may not be a great burden to the public, but many frequent fliers have pleaded for relief from lengthy preflight security lines and other security policies to which we all have become accustomed.

At the same time, I am in agreement with Administrator Hawley that our chief and ultimate responsibility, even beyond convenience—and I happen to be one of those advocating for convenience—is to have a balanced and direct and sure approach to the traveling public's security and how do we get there.

I believe that the Registered Traveler Program tries to strike a compromise between the goal of security and the freedom to travel. But I am willing to listen to the challenges that TSA faces and how we can address their concerns. This should be a meeting that everyone is as honest and as straightforward as they can possibly be. We can find a way if we find the honest pathway.

The Registered Traveler Program, in concept, is a worthwhile idea; it is, in fact, very simple. Frequent travelers will voluntarily submit to the background checks and give the TSA their fingerprints and an iris scan. The RT Program is a way for TSA to narrow its pool of potential problems; even if it is not popular, it will separate a small percentage of the people from the large stream of air travelers and give TSA an advantage in screening.

Each time I make those comments again, I am interested in a forthright discussion this afternoon. David Stone, the former Acting

Administrator of TSA, stated that the RT plan will provide frequent travelers with the means to expedite the screening experience without compromising on security.

I will be the first to tell you that there is not a perfect layer of security. There is no airport screening system that is 100 percent risk free, but the concept of the RT Program administered in a correct way could revolutionize the way security is administered. However, the RT program will be of limited value to participants if they have to, at this point, continue into secondary screening, at least having not gone through this hearing and hearing the reasons why such occurs.

I understand the RT Program is private-sector driven, but TSA can provide meaningful support, and I believe we can find a resolution. As much as I advocate for the technology, let me say I had the pleasure today of seeing it work. It is effective, and we should not ignore effectiveness; but as much as I view the program as effective, I want to be sure that it is secure. I believe that if TSA and the vendors work hand in hand, maybe we will have a successful product.

The RT Program is designed to improve the security process by helping TSA align screeners and resources with potential risks. Approved travelers will be positively identified at the airport through biometric technology. These passengers will go through expedited security screening, specially designated lanes in their home airport. Training, however, is key; and we must train the personnel, TSA and the private sector. I understand things will vary according to location as each airport will deploy different technologies and will have different security checkpoint configurations.

I want a system that all airports can use; I don't want a piecemeal pilot program. If we are to move forward on this particular program, I think it is important that we find a way to make it work.

The second most important is security, after convenience. Since more is known about RT users, TSA screeners will be able to focus their efforts more effectively. Customer service has been mentioned first; I think I would like to change the order and indicate that security must be first.

The Chair now recognizes, as I close, the ranking member of the subcommittee, the gentleman from California. And let me simply say, as I yield to him, this hearing should be about solutions, working together and about securing America. With that, I yield to the distinguished gentleman for an opening statement.

Mr. LUNGREN. Thank you very much, Chairwoman Jackson Lee.

I want to welcome Assistant Secretary Kip Hawley. You have been an outstanding leader for the Transportation Security Administration. You have been confronting our transportation systems after 9/11.

I also look forward to hearing from our private sector witnesses, concerning their experiences with the Registered Traveler Program and how we might actually get it working nationwide.

I believe RT is the kind of innovative security program we have been encouraging the private sector to develop. We have said the government can't do everything; we ought to utilize the private sector when they have expertise that we cannot duplicate. We would

like to see a partnership between the private sector and the government.

I must say, I have been disappointed with the lack of rapidity that we have seen in the development or approval of this program by TSA. I just, from the beginning, thought the Registered Traveler Program makes sense. Those who are frequent travelers are willing to pay a premium to have less hassle, to not have to worry whether they are going to have a line that is an hour, hour-and-a-half long. And it seems to me, if we are trying to be effective in terms of screening passengers, we need to reduce the size of the haystack.

One of the ways of doing it is getting people who voluntarily give us more information than otherwise would be available; and certainly, giving us a confirmable biometric is important. This is done voluntarily: They give us their thumbprint, they can have an iris scan, they have a picture already on file. We saw all those things combined in the kiosk that is over on display in the Longworth Building today—along with its ability to check shoes while they are still on your feet, I would like to add. I just think that makes sense.

If I were to step back and try to develop a program, it seems to me that is the kind of program I would like to develop. That is why I am concerned that with all the innovation that I have seen come out of TSA and all the flexibility, this appears to be an area in which there has been an amount of inflexibility; and I am disappointed with that. I think we can facilitate movement through airport screening areas while maintaining a high security level. We would benefit TSA, the airlines and their passengers.

The other thing is, if we can reduce the lines and have people move through those lines faster, you reduce the security risk that is inherent at the airport itself where you have a congregation of passengers and employees. We saw what happened at the Glasgow Airport. They certainly weren't going to get to a plane, but they were going to get to passengers and other infrastructure right there. So anything we can do to actually expedite the movement of people makes sense.

So I want to see the public-private partnership working together. I want to see it as harmonious as possible. And I am very much looking forward to hearing the testimony of Mr. Hawley and those others who are in the development stage and implementation stage.

We now have tens of thousands of people using it. We have had the pilot project for a number of years at a number of airports. At some point in time you have to say, the program is going to work or not going to work.

I know you folks get tired of me saying this, but man, we moved faster from the beaches of Omaha and the other beaches there at Normandy, through to Berlin, than we have in going through the pilot project for Registered Traveler; and I don't understand why we should have any more delay.

The one positive I see is, the recent development of Registered Traveler interoperability standards is what we have been waiting for. I am glad that we have it now, and I am glad we have those standards against which the program and the equipment are going to be measured. So I would just hope that we can move on this,

and I hope that the testimony today will give us some idea where we are in this line, how much more needs to be done; and if there are problems, administratively or legislatively what we need to do to fix them.

With that, I yield back the balance of my time.

Ms. JACKSON LEE. I thank the gentleman for his remarks.

Let me remind my colleagues that other members of the subcommittee are reminded that under the committee rules opening statements may be submitted for the record.

Ms. JACKSON LEE. Votes have been called, but I am going to yield to the Administrator for his opening remarks. I would like to welcome Kip Hawley, the Administrator for the Transportation Security Administration at the Department of Homeland Security.

We would like to welcome you back, and we have many challenges before us, of course.

We would like to give you an opportunity before the members go to vote—or some may go, but we would like to give you the opportunity to present your testimony.

Without objection, Administrator Hawley's full statement will be inserted into the record. And I ask that you summarize your statement in 5 minutes.

**STATEMENT OF HON. KIP HAWLEY, ASSISTANT SECRETARY,
TRANSPORTATION SECURITY ADMINISTRATION,
DEPARTMENT OF HOMELAND SECURITY**

Mr. HAWLEY. Thank you. Good afternoon, Chairwoman Jackson Lee, Ranking Member Lungren and members of subcommittee. Thank you for the opportunity to put the Registered Traveler Program into context. I think the comments the chairwoman made about Phoenix underscore the many serious issues before us in aviation security.

In putting the Registered Traveler Program in context, I think it is important to note that that context is dominated by today's threat environment. Two weeks ago the National Intelligence Estimate confirmed publicly what members of this committee have known for quite some time. We are under heightened terrorist threat; it is real, and it will not go away soon.

We know of continued terrorist interest in attacking the aviation sector. We know of training in the use of improvised explosive devices. We must account for the possibility of terrorist dry runs, and effects of the so-called "clean skinned" terrorists, those not known to the authorities who have no obvious, identifiable risk factors. I21Madam Chairwoman, Mr. Lungren and members of the committee, you have made this committee's expectations very clear to me, that TSA must focus its resources on the highest priority efforts against the active terrorist threat. We share the same priorities, partner with others to help stop threats at their earliest stages, and by our own actions, deter and disrupt this adaptive enemy whose goal is mass casualties and dramatic destruction. That is the real problem we face every day.

The threat is real. TSA's responsibility is very real, and the question is, how does RT fit into that picture?

We all want to go through faster with less hassle. We know that we are not the terrorists; why waste time screening me? A pas-

senger goes through screening knowing that he or she is low risk, and it is logical to think that there has to be a way not to waste resources screening me. The crux of the problem is how we define “we” and “me.”

Just us relying on frequent flier miles isn’t enough. In the age of the “clean skinned” suicide bomber, just the absence of a negative is no longer enough. Once we define “trusted,” that provides a blueprint for vulnerability, and a security risk introduced at RT becomes a risk for every passenger, because what we make easy for one becomes easy for many. We need many layers of security to mitigate the risk of defeating anyone. We want to increase the level of security, not decrease it.

After prioritizing our security initiatives, based on risk, TSA decided the taxpayer resources are best applied to more critical needs than Registered Traveler: explosive detection training, a better quality workforce through better recruiting, higher retention, pay for performance, career progression, additional layers of security and behavior detection, VIPER teams, document checking, employee screening, daily checkpoint explosive detection drills, better intelligence integration, proactive Federal air marshal missions, secure flight, checkpoint process improvement, harmonization of international security measures, more effective use of existing affordable technology, active engagement with our partners in terms of security, general aviation, rail and port security, better vetting of those with access with critical infrastructure to name just several highlights. These are the security measures that help protect against the threat we know we face.

In the context of these other activities, RT is not now an effective operation tool against the “clean skinned” terrorist; therefore, we have not reduced the security process for RT passengers. There is lots of room for innovation that doesn’t lower security, doesn’t cost the government money or doesn’t burden extra passengers. However, TSA is not waiting for RT; we are moving forward to improve the security process for all passengers.

As I announced last week, we are reviewing the checkpoint process to make it less dependent on the 25-foot by 15-foot box at the checkpoint. We understand that the legacy process appears to pit TSA against the passengers by jamming us into a small space and launching 2 million passengers a day through the magnetometers at us. We can improve security and make the process smoother by spreading out security, calming down the environment and changing our security measures. I am hopeful RT can play a role in this effort.

Thank you for an opportunity to discuss these issues, and I will be happy to answer any questions.

[The statement of Mr. Hawley follows:]

PREPARED STATEMENT OF THE HONORABLE KIP HAWLEY, ASSISTANT SECRETARY,
TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND
SECURITY

Good afternoon, Chairwoman Jackson-Lee, Ranking Member Lungren and members of the Subcommittee. Thank you for this opportunity to speak with you regarding the progress the Transportation Security Administration (TSA) has made in implementation of the Registered Traveler (RT) program, currently in its pilot phase.

The Aviation and Transportation Security Act (ATSA), P.L. 107-71, charged TSA with protecting the Nation’s transportation systems while facilitating the movement

of people and commerce. TSA is committed to providing comprehensive security to our Nation's transportation systems. At our Nation's airports, TSA has implemented a risk-based, multi-layered approach in order to efficiently allocate scarce security resources and institute redundancies in the system to thwart potential attacks. We know that where aviation security is concerned, there is no single silver bullet that will protect against all threats. Moreover, aviation security exists in an ever-changing security environment requiring TSA have the flexibility to change procedures and requirements quickly to respond to new threat assessments.

This has never been more clearly evidenced than by the prohibition on liquids implemented across U.S. airports in the aftermath of the foiled transatlantic terror attack of August 10, 2006. In less than one day, TSA was able to implement a completely new security regime nationwide. Just a few weeks later, after a thorough evaluation of the potential threat, we were able to reevaluate those procedures and allow some liquids in passenger carry-on baggage. We are only able to quickly respond to newly discovered threats because Congress has given us the discretion to adapt our security programs as necessary. We use that flexibility every day through unpredictable security procedures designed to counter constantly changing threats, known and unknown. It is imperative that we maintain this flexibility as we move forward with any change in airport security, including a developing RT program.

It is against this backdrop that TSA's RT program and its development and implementation must be understood and evaluated. Section 109 of ATSA authorized TSA to "[e]stablish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening." It is important to note a number of things about this authority. First, Congress understood in establishing this authority that a trusted traveler program, although not critical to security, is a program that may be beneficial to the traveling public and could complement TSA's layered approach to aviation security, allowing TSA to focus resources elsewhere. Second, Congress recognized that any trusted traveler program would be dependent on the availability of appropriate technologies.

Essentially, the RT program is a privilege program that, if fully operational, would offer a streamlined security experience for applicants who pay a fee and meet both TSA and the Service Provider's eligibility requirements. RT would provide benefits to participants while encouraging commerce, safeguarding personal privacy, ensuring a self-sustaining program, and enhancing the protection of the traveling public, all without disadvantaging the general public when they fly.

Currently, RT is a public/private sector partnership pilot program, supported and overseen by TSA, with distinct roles and responsibilities for each participating entity. TSA is responsible for setting program standards, conducting security threat assessments of participants, performing physical screening of RT participants at TSA checkpoints, testing new technologies prior to implementation, and other forms of oversight. The private sector Service Providers are responsible for enrollment of RT participants, verification of participants' RT status using biometric technologies at RT kiosks, and related services. Participating airports and air carriers oversee their Service Providers and ensure that those Service Providers comply with the requirements of the RT program. As part of a complex, layered security scheme, RT may operate differently at each participating airport, within the broader security plan of the airport.

Registered Traveler Yesterday: A Brief History of Program Development:

Mindful of the challenges and potential of RT, TSA first undertook an elaborate pilot program to explore technology, customer reaction, and private collaboration in the development of a comprehensive, nationwide RT program. This pilot was funded by the Federal Government. During the summer of 2004, the Registered Traveler Pilot Program was initiated at five airports on a staggered basis around the country. This initial pilot ended in September 2005.

In June 2005, TSA initiated a new pilot, also funded principally by the Federal Government, known as the Private Sector Known Traveler, at Orlando International Airport (MCO), to test the feasibility of a public-private partnership model for the RT program. The initial successes of the pilot programs demonstrated that the biometric verification technology can work under airport operational conditions and that the public is willing to pay a participation fee and accept private industry involvement.

Following the Orlando pilot, TSA worked with private industry to roll out an expanded public-private partnership pilot to test interoperability among multiple service providers. Public expectations were raised by the pilots and the appealing origi-

nal notion that vetted travelers could be sped through security while higher risk passengers received more scrutiny.

After my confirmation at TSA in late July 2005, I began a reassessment of TSA's security priorities based on Secretary Chertoff's risk-based approach to security throughout the Department. It was clear to me that TSA needed to apply its resources to achieve greater capability to stop attacks using explosives brought on an aircraft by terrorists. The Committee is well-familiar with the extensive progress that TSA has made in that effort. TSA has made significant progress in targeting our procedures towards specific threats and enhancing our workforce. Our Transportation Security Officers (TSOs) now receive enhanced training in detecting components of improvised explosive devices.

We are also taking action to demonstrate our increased confidence in our TSOs. In July 2006, we announced that the TSO position was being reclassified to a specialized job series, in recognition of the nature of the work they do. In addition, we rely heavily on TSO input through the National Advisory Council, which represents TSOs throughout the nation on workforce issues. We have created an additional forum through our Idea Factory to promote workforce ideas on any number of topics, from technology and detection to quality of life issues.

As much as the RT concept appeals to all of us, it would be security folly to reduce security based only on the lack of prior criminal or discovered terrorist activity. The reality of the "clean skinned" terrorist—a terrorist without criminal history or identification on a watch-list—was made abundantly clear in July of 2005 when such terrorists attacked the London transit system. After prioritizing our security initiatives on a risk basis, TSA decided that taxpayer resources were best applied to more critical needs than RT. However, given the extraordinary public interest in the program, and the appealing logic behind it, TSA was willing to give wide latitude to private sector entrepreneurs, airlines, and airports if they were able to construct an RT program that did not increase risk to the system. It was this private sector-led program that TSA announced in February of 2006.

Private sector partners stepped up and organized themselves to set interoperability standards approved by TSA in May of 2006. This process took longer than initially expected, but produced the notable result that RT and TSA now have access to an interoperable biometric credentialing system, built in less than a year, and at no cost to the government.

Rather than wait for an entire rule-making process before testing this new system, TSA and the industry began a pilot, known as the Registered Traveler Interoperability Pilot (RTIP). TSA released the RTIP Fee Notice in the Federal Register and developed a comprehensive set of guidance documents allowing the private sector to implement the interoperability pilot phase. The initial fee of \$28 per participant covers TSA's costs for vetting and program management. Any additional services or costs associated with RTIP will be established by the vendor, who may, in turn, charge the participant for those services. This expanded pilot is designed to ensure the interoperability of biometric cards among multiple services providers at different airports across the country.

The interoperability pilot began in January 2007, when the first airports/air carriers were approved by TSA to provide RT services. With the addition of Reno/Tahoe International Airport and a second active RT vendor in May 2007, TSA is closely monitoring RT interoperability to ensure that participants of one vendor can seamlessly use RT services provided by another vendor. This is a key component of RT that must be fully functional prior to launching the program nationwide.

Currently, seven airports and three air carriers are participating in the RTIP in nine locations. Four airports and one air carrier have initiated agreements with a Service Provider but are not yet operational, and four airports are currently soliciting Service Providers for RT. TSA has approved five Service Providers, with three currently offering active service and five more are in the approval process.

Registered Traveler Now: An Overview of the Current Program

RT, still in the pilot phase, is an entirely voluntary program; airports have the option to utilize the program and passengers may voluntarily sign up for the RT service. At airports that choose to offer the RT service, TSA is intimately involved in ensuring that any RT service offered has no negative impact on the security of passengers traveling through the airport. TSA and the airport work closely together to ensure the overall security plan of the airport is updated and provides robust security to the flying public.

While TSA will largely play a facilitating role, the private industry is responsible for market definition, program benefits, and interoperability. TSA-approved vendors are responsible for marketing the RT program to the general public, signing up participants, collecting enrollment fees, and providing verification services. Vendors are

also responsible for working with airport authorities to modify airport configurations to minimize wait times, enhancing customer service, partnering with airport concessions and services to provide membership benefits, and investing in new technologies to facilitate security screening.

As part of the RT program, TSA uses participants' biographic data to conduct threat assessments against terrorist-related, law enforcement, and immigration databases that TSA maintains or uses, and ensures that participating airports maintain effective security procedures. As private vendors innovate, explore and seek to incorporate new technologies, TSA must ensure that each system is subject to rigorous testing. TSA will ensure that implementation of new technology does not compromise security.

Passengers using RT checkpoints today walk up to a biometric reader, place their card in the reader, and present their biometric (fingerprint or iris scan) for verification. Once their current RT participation status has been verified, they can then proceed directly to TSA screening where they will go through the same screening process as all passengers. In most cases, RT participants use an integrated lane and may go to the head of a screening line.

A recent issue raised by the RT community is TSA's requirement that RT members, like all commercial aviation travelers, show government-issued photo identification when their boarding passes are inspected at security checkpoints. Based on the current aviation threat level, TSA views this step of the screening process as an essential layer of transportation security and the best way to provide assurance that the passengers presenting themselves at security checkpoints are the passengers identified on their boarding passes. Further, the configuration and location of RT verification kiosks, in relation to the security screening checkpoints, varies in different airports. Lack of control over the ingress to both screening and the secured area is a practical factor with possible security consequences. When establishing nationwide program standards, TSA must consider differing airport and vendor models. Despite these concerns, we believe that, under certain circumstances, TSA may be willing to accept RT cards in place of government-issued ID cards. For example, we have stated that if all RT Service Providers adopt a card protocol requiring photographs, legal names, and appropriate security features, we would reconsider our position. However, the Registered Traveler Interoperability Consortium (RTIC), which includes all five TSA-approved Service Providers, has decided through consensus not to add this requirement to the technical interoperability specification governing their mutual operation of the program. In alignment with the public/private partnership model for the RT Program, TSA will continue to act in an oversight role, and allow private industry to agree upon standards for business and technical interoperability. In short, if the RTIC collectively decides to implement a photograph and other security measures on the standard RT card, we are willing to consider accepting an RT card as sufficient identification to pass through TSA screening.

It is important to note that the RT program is still in its pilot stage, and TSA is continually assessing security and operational issues to determine whether changes to the pilot are necessary. The market, through participating airports/air carriers and Service Providers, will help determine the future shape and scope of RT by recommending new technologies and practices that provide an equivalent or higher level of security and service compared to current procedures which TSA will evaluate based on the guiding principles of RT.

Registered Traveler Tomorrow: Where We are Going

As the interoperability pilot matures, we expect to begin the rulemaking process to further define RT. We will use the lessons learned in implementing the RTIP and feedback from RTIP participants and partners to develop necessary regulations. Initial benefits of the RT program may include modified airport configurations to minimize RT passenger wait times, enhanced customer service for RT participants, such as divesting assistance, concierge service for luggage, parking privileges, and discounts for service or concessions. We expect benefits to be defined as the private sector identifies and invests in innovations.

While working to facilitate where the market may take RT, we must also consider that the number of RT passengers flying on a given day is likely to be only a small portion of the travelers who pass through TSA security. The total membership in the RTIP is 39,000. To put that in perspective, if the entire current enrollment of RTIP were to fly every day of the year, RT passengers would amount to less than 2% of the 2 million passengers screened by TSA. We are working to ensure that as the RT program matures, we are not disadvantaging the general public.

TSA is excited about the technological innovation potential of RT and is already seeing the benefits of the biometric credentialing system; some technology companies have already begun to bring new security innovations to us for testing. We are

working with those entities to provide testing, including laboratory testing, and feedback as products develop. The critical factor in developing technology is that it work seamlessly with security protocols and that it not compromise security in any way.

To this end, TSA has a consistent process for the evaluation and testing, acquisition, deployment, and operation and maintenance of security technologies procured by the agency to meet a mission need. Since its inception, TSA has utilized this process with multiple vendors and believes vendor responsiveness and technology maturity significantly contribute to the approval process. In response to the RT program and the introduction of security technologies designed for an accelerated access control lane for passenger screening, TSA has developed a similar process that permits the rapid but thorough testing of any equipment proffered by the private sector to substitute for current security protocols. This process provides assurance to TSA that the technology introduced into the RT program will not compromise security. In short, we are committed to facilitate the rapid deployment of technology to RT participants once we know that the technology will achieve its objective and that its implementation will not diminish security.

We hope to see new improved technology in the market as RT matures, and look forward to continued technological success from private industry as they search for ways to make the RT service more successful. TSA will continue to work with the RT community and our network of airports and air carriers to advance our mission of securing our Nation's transportation network.

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 question you may have.

Attachment:

Airlines involved in initial RT pilot (4):

Northwest Airlines
United Airlines
Continental Airlines
American Airlines

Airports involved in initial RT pilot (5):

Minneapolis-St. Paul International, MN
Los Angeles International, CA
George Bush Intercontinental/Houston, TX
Logan International, MA
Ronald Reagan Washington National, VA

Locations currently operating RT programs (9):

Albany International, NY
Cincinnati/Northern Kentucky International, KY
Indianapolis International, IN
Jacksonville, FL
John F. Kennedy International, NY
(Virgin Atlantic, British Airways, and Air France)
Newark Liberty International, NJ (Virgin Atlantic)
Orlando International, FL
Reno/Tahoe International, NV
Norman J. Mineta San Jose International, CA

Airports currently in agreement with a service provider, but RT is not yet operational (5):

Air Tran at LaGuardia International, NY
Greater Rochester International, NY
Little Rock National, AK
San Francisco International, CA
Westchester County, NY

Airports currently soliciting service providers (4):

Hartsfield-Jackson Atlanta International, GA
Denver International, CO
Ronald Reagan Washington National, VA
Washington Dulles International, VA

Approved Vendors (5):

Fast Lane Option Corporation (FLO)
Unisys Corporation
Verant Identification Systems, Inc.
Verified Identity Pass (VIP) (CLEAR)

Vigilant Solutions

Vendors Seeking Approval (5):

Priva Technologies, Inc

Fly Fast, LLC

PKM Music, LLC

DSCi

VIP Alaska

Ms. JACKSON LEE. I thank the Administrator, and I would like to call for a recess for the votes. And we will return. This is going to be eight votes. I don't want to send out the TSA employees to find you. Please be relaxed, and we will return as soon as we can. Thank you very much.

The hearing is in recess.

[Recess.]

Ms. JACKSON LEE. The hearing will come to order.

Might I thank the Administrator again for his insightful testimony?

At this time, I remind each member that he or she will be granted 5 minutes to question Panel I, and I now recognize myself for questions.

Let me first of all acknowledge, Mr. Hawley, that as the ranking member indicated, we thank you for your service and those of us in this committee have to be on the same page as relates to the security. I think the jurisdiction of this subcommittee has one of the greatest components of impacting the public. The public is constantly using either critical infrastructure or some form of transportation, even as we speak today.

So we certainly agree with your concerns about security, but we also are interested in efficiency, effectiveness and the, if you will, corraling of resources globally to be effective in our security.

Give me the challenges that you foresee with an expanded Registered Traveler Program. And wouldn't it seem logical that if we can find a better mousetrap, a more refined technology, that that speaks to both of our concerns, which is a secured homeland and an impenetrable system that can help us in the flow of people and commerce?

Mr. HAWLEY. Yes, ma'am, I think that is exactly right. There is a lot of promise in technology as being able to accelerate this program. I think Registered Traveler has great promise in the future. It has already delivered a biometric credentialing system that is interoperable, that is a great thing.

The technology is not yet there to provide significant screening benefits to the RT members, but I am confident that as technology develops, that will occur. At least one technology provider has already stepped up and is working with us to try to provide an answer that would allow folks to keep on their shoes, if that works. But I see that as a way forward.

Ms. JACKSON LEE. What made you believe the technology is not there?

Mr. HAWLEY. Our testing—and I may not be able to brief you on a classified basis as to why that is the case. Just because it is not ready for prime time now, I am confident that GE will develop a program that we can use.

Ms. JACKSON LEE. Let me go particularly to Orlando where, for a period of time, you did not require a picture ID; however, subse-

quent to that, it seems that you began to require a picture ID. In a letter dated July 2nd from Jeffrey Sorrell, he wrote that a government-issued photo ID is the best way to provide assurance that passengers who present themselves as individuals are identified on the boarding passes.

Now, I know that having experienced a pilot of the technology, a printout comes out with your picture on it that you can certainly identify, but why did TSA suddenly require these RT numbers using RT lines to show a picture ID and an RT card before entering the line?

Mr. HAWLEY. Because it is going to be a national program and needs to be interoperable. And the airport in Orlando is well configured for a Registered Traveler, but it has to be interoperable at all airports; and if the power were to go out, for instance, and the printer would not work for some reason, having a valid federally issued photo ID, we believe, has significant security benefit.

Ms. JACKSON LEE. Do you remain open to—you have indicated that you foresee improved technology. Do you foresee the improved technology where you will not ask for the independent photo ID?

Mr. HAWLEY. Well, we work with the Registered Traveler Interoperability Consortium for whatever interoperable standards are for Registered Travelers, so we are open to that. We just want to have one that, if we are going to use a photos, it be secured.

Ms. JACKSON LEE. Do you see using a photo on the RT card? I understand TSA has suggested that in the past as an option?

Mr. HAWLEY. That is an option, but we need it to be an interoperable one where all cards are subject to the same security standard.

Ms. JACKSON LEE. Because if a card were revoked, someone would still be carrying around the card with the picture and so that would negate what you want it to do?

Mr. HAWLEY. Correct. Potential vulnerability.

Ms. JACKSON LEE. Let me see if you are prepared to accept the viability of the technology, but you are asking to have added measures of enforcement or security along with this technology.

Are you today saying that the Registered Traveler Program is not a program that you feel is sufficiently secure?

Mr. HAWLEY. The current—if we are talking about technology in Orlando, we have other measures in place to protect the public. However, more widespread use of that machinery would not be realistic from a staffing point of view, and it alone does not provide the protection we require at this point.

Ms. JACKSON LEE. I don't think the technology will substitute for, obviously, the overall screening. But if you have the ability—you shared some thoughts with me in a private briefing about efficiency and effectiveness. If.

You have an ability to vet individuals so that a certain small percentage of travelers are able to go through because they are vetted, known, doesn't that give more opportunity for a greater focus on the overall war on terror, that we have to confront those unknown, unexpected, precipitous actors that are out there ready to act at any moment?

Mr. HAWLEY. That is certainly possible.

Today, I would highlight that Registered Traveler members have only the terrorist watch list check. So today it is just that, which I don't consider enough. In the future, it could be more, and that would change the equation potentially.

Ms. JACKSON LEE. Say that again. I am sorry.

Mr. HAWLEY. The current RT card is only subject to the terror watch list check, nothing more. And in the future, it is possible, as you mentioned in your opening statement, as did Mr. Lungren, that if people give more information, a further assessment can be made.

Today, it is just the watch list check, and the industry has declined to go further and do the background check. So since, as you know, the issue of government dealing with commercial data is off limits for us, we are not going to go there.

And it was something that we discussed with the industry earlier on, that they would do the background checks that would then allow us to make security benefits. They elected not to do that, so I am just left with a terror watch list as the only check done with the biometrics.

I know I fingerprinted somebody who is not a watch list member, but that is it.

Ms. JACKSON LEE. My time is far spent. Let me thank you for your testimony.

You are not closing the door on this technology, however?

Mr. HAWLEY. No, no. We think it is promising.

Ms. JACKSON LEE. Thank you.

I am pleased to yield to the distinguished ranking member 5 minutes.

Mr. LUNGREN. Thank you very much.

Can you tell me what the premium line program is at Dulles?

Mr. HAWLEY. I believe that is controlled by the airlines. TSA takes over where someone submits themselves for screening; and under the current arrangement, that is a function between the airline and the airport to do.

Mr. LUNGREN. So they are not prohibited from doing that?

Mr. HAWLEY. No.

Mr. LUNGREN. I am trying to understand, because I have supported you on most of the things you have done, and I think you are doing a very good job. But I am trying to understand whether the support for the RT Program has fallen out at TSA, and has there been a reassessment of the RT Program such that TSA is no longer supportive of it.

Mr. HAWLEY. No. The issue is the "clean skinned" suicide bomber. And as I just mentioned, the only thing we have is the biometric on an individual who is not on a watch list, which doesn't make me feel comfortable in the world of the suicide bomber, we know they are interested in dealing with modified electronics.

Shoe bombs remain a current concern, and a body carrying explosives is a method. So shoes, coats and laptops can't be off the screening table just based on an absence of a watch list.

Mr. LUNGREN. If the technology exists—I saw this kiosk over there; I don't know whether it works or not. It looked like it worked.

Let us suppose it does do what it says it does, with GE, that identifies the presence of metal in a shoe or the presence of some combustible material that you don't want on a plane; wouldn't that be something, in addition to the biometric, that is beyond what is done to those who go through the regular line today?

Mr. HAWLEY. Yes, sir, when it works up to standards—and we have provided those to GE; they are well aware—we will be delighted to accept it. The problem is—

Mr. LUNGREN. Are these the standards that came out a couple days ago?

Mr. HAWLEY. Yes. Although we said, for 6 months we have been talking about this and when it reaches the point of being able to satisfactorily detect explosives, we will be delighted to have it. It is not at that point today.

Mr. LUNGREN. But those are—the standards that came out this past week are the ones against which the machine will be judged?

Mr. HAWLEY. The detailed specs are, but up—it has never detected explosives to our satisfaction, even close. Now that they are getting close, we have refined exactly what the bar is and agreed on that.

Mr. LUNGREN. And, of course, seeing whether or not the presence of metal is in the shoes, correct?

Mr. HAWLEY. Sure, there has to be improvement there as well.

Mr. LUNGREN. If those met your satisfaction, that would be something in addition—I mean, that would at least give you the same level of review that you are getting by people going through the line and taking their shoes off and so forth, correct?

Mr. HAWLEY. We would be delighted, and we would enthusiastically support that.

Mr. LUNGREN. Does not the biometric allow you to identify the specific person, as opposed to everybody else going through that shows some sort of ID?

Mr. HAWLEY. It is great identity validation and—yes.

Mr. LUNGREN. Correct me if I am wrong, but I understand that right now, if you are under 18 years of age, you are not required as you go through the regular line to show a picture ID; is that correct?

Mr. HAWLEY. Yes.

Mr. LUNGREN. I was told you are requiring that for people going through the Registered Traveler line?

Mr. HAWLEY. For underage people, I frankly don't know the answer for that, I would be happy to check on it for the record.

Mr. LUNGREN. If that is so, I would like for the record, if you could tell us why that makes sense. It doesn't seem to make sense to me, if you don't do it going through the regular line, you would do it through the RT line.

There has been a question in the past as to what benefit someone would get from going through the RT line. It seems to me that—obviously, I don't have to take my shoes off; if I am going through a line that is probably somewhat shorter because you have that ability not to take your shoes off and just go through this—that is something I would want to do.

Is there any limitation with respect to people who—vendors who are coming up with the RT Program on what they could offer? Be-

cause we had this debate before, whether they could bundle it with other kinds of benefits.

Mr. HAWLEY. Yes, sir. In Amsterdam, there is a thriving program analogous to it where—it is a wonderful program, and they do nothing on the security side; they do a lot of innovation elsewhere. We have offered on-line reservations, off-site checking, the background checks; there are a number of things that are open now today without us changing any of the security.

Mr. LUNGREN. Would you indulge me for one moment, Madam Chair?

Ms. JACKSON LEE. Without objection.

Mr. LUNGREN. I would like to ask you one question about the background check, because this is very, very important.

TSA ran into a little bit of trouble a year and a half ago when you had outside information that you were not going to look at; and then someone said that you did look at it. I don't know what that whole argument was about, but the question was, if we were going to identify people who are on the watch list versus people who have a similar name on the watch list, the best way to identify them and exclude those who should not be on the list was more information.

There was some fear—some civil libertarians had, some privacy experts had—that if we gave more and more information to government, here comes 1984.

So the issue was, is there a way that you can have a system whether you query commercially held data by the private sector. Analogously, would you support a program or is there a problem with the program where the vendor actually asks for more information such that not only is the biometric going to qualify that document as being with the person who holds it, but also so that you have better information on who that person is.

Mr. HAWLEY. Yes, sir, that would work.

Our thought is that we would verify the process by which the private sector entity would do a background check, as they do in financial services. If we just got a red light, green light, and could audit the process, then we would grant commensurate security benefit.

Mr. LUNGREN. Thank you very much. Thank you for your indulgence.

Ms. JACKSON LEE. The gentlelady from the District of Columbia, Ms. Norton, for 5 minutes.

Ms. NORTON. Thank you very much for this hearing, Madam Chairman.

I see at the top of the news almost every day, they are reporting the combination of whether economic canceling—it is a wreck; I am on the Aviation Sub, it is a wreck. I must say, TSA is doing the rest of what needs to happen to drive the airlines out of business, sir.

I want to say to you, straight out, that your testimony—I am going to read from the parts of it—gives me real doubt that you are being fair to the security needs of the country, that you are being fair to the public, that you are being fair to the innovators, or that you are being fair to this committee. And I want to be just as straight as I think your testimony has not been straight with us.

I believe that the one thing we probably can depend upon, given what I know as a member of the Aviation Subcommittee about what your TSA personnel are not finding, the one thing that I think is a failsafe is failsafe innovation in security such as optical scanning.

Let me tell you why I believe your testimony casts doubt on whether or not these people should continue to put any more money in that program. A security risk introduced—page 2 of your testimony—with RT becomes a risk to every passenger; we need layers of security to mitigate the risk of defeating one. We want to increase the level of security, not reduce it.

That says to me RT-plus.

You go on to say, there is lots of room for innovation that doesn't lower security. What are you talking about? Or costs the government extra or burdens other passengers, as if you are casting aspersions on RT. And you go on, just in case we think you are serious about RT, to say, TSA is not waiting for RT. We are moving forward to improve the security process for all passengers.

Sir, I have seen what you have done for all passengers, using TSA workers as your form of security. And I just have to say to you, I don't see anything in this testimony to give this committee or the people who are throwing money into innovation any hope that you will ever let—particularly given the way you have been slow-walking, testing until we announced this hearing, that you are ever going to let anything happen here.

And when you talk about "clean skinned" terrorists, the "clean skinned" terrorist that I am most afraid of the public for, the ones who can get through the screening that you have now while you stand in the way of innovation.

My question to you, sir, is, why should anybody put another dime into this innovation with what your testimony says about how you think, to quote you, "RT isn't ready for prime time," TSA has decided that taxpayer resources are best applied to more critical needs than RT. Sir, that is telling these people to go fly a kite. And I think that the notion, given your record with what you are doing, that you would say to innovation, there is no hope for you, is a total and disgusting insult.

That is my question, and I need you to assure me that this is worth their time and money, because if I were in their business, I would not read your testimony as saying that it is.

Mr. HAWLEY. I think a function of leadership is to make decisions and particularly about resources and priorities. And in a security world, I listed previously in my testimony a number of our priorities and the fact that Registered Traveler is not ahead of those other programs in priority is not a slam on it. In fact, the program is self-funded, so I am not asking for money out—

Ms. NORTON. So what do you want, what would you like them to do next?

Mr. HAWLEY. I would like to use equipment that works, and work with them on—

Ms. NORTON. Why don't you test the equipment they have?

Mr. HAWLEY. Ma'am, we have.

Ms. NORTON. You have done no such thing. You are just beginning to do real testing of this equipment, of it—you were sworn, Mr. Hawley.

Mr. HAWLEY. That is correct. That is not an accurate statement that we have, in fact, tested the device; and there are shortcomings, and we expect them to be corrected. Once they are corrected, we would be very pleased to have them be a part of the security process.

But I think the part you quoted me saying is absolutely accurate. If we let a vulnerability exist in Registered Traveler, that passenger who could be a threat is out there and can be a threat to every passenger in the system. So we have to have RT not create security vulnerabilities, and we are comfortable that RT will mature and not be in the position of jeopardizing other passengers.

Ms. NORTON. Mr. Hawley, finally, just could I say, do you realize, why this committee is having a hearing and why there will probably be a hearing in the Aviation Subcommittee as well is precisely because of delays at TSA? If this is supposed to be an administration that is for innovation, you are the poorest excuse for innovation I have ever seen come before the Congress; and shame on you for what your slow-walking of this innovation, saying yea or nay, is doing not only to the airlines, but to the general public, and I submit to you, your candor before this committee.

Thank you, Madam Chair.

Ms. JACKSON LEE. Gentlewoman's time has expired. Thank you, Congresswoman.

Let me yield 5 minutes to the distinguished gentleman from Georgia, Mr. Broun, for his questioning.

Mr. BROUN. Thank you, Madam Chair.

Mr. Hawley, I just have a couple of quick questions. You testified in your opening statement that your RT is not ready for prime time. Any idea about how close we are to having some idea about when it might be ready?

Mr. HAWLEY. A lot depends on the private sector innovation and coming forward with attractions for the customer. Those are things that are well within the private sector and, as I just mentioned, are not priorities for us to divert resources over, to figure out how to make it more marketable. So, as additional technology is applied and can offset security measures, we are pleased to have them in. As I mentioned, we are not in a position where we are able to prime the pump, so to speak, to help RT at the expense of the general passenger.

Mr. BROUN. Okay. I frequently travel out of three different airports. One is my hometown of Athens, Georgia, where RT is not going to make any change at all in—when they needed expense for that community.

I also fly in and out of Billings, Montana; and frequently there I run into security lines that may be 30 minutes or longer. And Atlanta may be a whole other question. The economic status of those communities and those States is quite different also.

I was just wondering, is the cost effectiveness for a community and the ease with an RT passenger getting through, is this something that a place like Billings, Montana, could put into place and

something that would ease the pain of having to stand in lines in places like that?

I understand Atlanta will be completely different. I would like to hear comments of what you have in mind about that.

Mr. HAWLEY. Yes, sir, for Billings, Montana, and Athens, Georgia, and small communities you don't need to have a fully vetted RT Program, there are other ways to do innovation, if you want, at the checkpoint. We are open to that kind of thing. The half-hour wait is an exception, and we—by and large, if we are staffed up at the time that the rush hits, then it is a question of the physical capacity of the checkpoint so our responsibility is to fully staff checkpoints in advance of when the rush hour is.

Now, Atlanta is a particular challenge for us and the airport director has been in touch with me, and we have tried a number things that bring the lines down low. They have a particular—one checkpoint situation that, if it gets behind, is a big problem. So we now have committed to open those lanes in the morning in time to process the maximum through the physical—outlay.

Mr. BROUN. Thank you, Mr. Hawley.

Ms. JACKSON LEE. I thank the gentleman for his questions. Do you yield back?

Mr. BROUN. I yield back.

Ms. JACKSON LEE. Now may I recognize the distinguished young lady from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Madam Chairwoman. And thank you for holding this hearing, which I think is an important one.

Every Monday I walk by the RT Program in the San Jose Airport, and because I do—and sometimes I get there way early—I checked it out, and I didn't actually join the program yet. It seemed to me there was a lot of smartness about it. You have 10 fingerprints, something that many of us have been suggested for a long, long time; and I was—one of the things we know in biometrics is that a positive ID, there is no faking it.

And so I was really surprised when I learned that the TSA is, in addition to the biometrics, requiring a photo ID on some government card. And it seemed to me that the TSA was saying that, you know, your student body card is a more reliable indicator of identity than 10 fingerprints and an iris scan. Is that the Agency's position?

Mr. HAWLEY. We do require a government-issued photo ID and that is, as I mentioned in the previous question, in case the power goes out.

Ms. LOFGREN. I don't want to be—as you—I like you very much and think you have done some good things at the Agency, but that is a preposterous thing to say. If the power goes out, everything goes out.

Mr. HAWLEY. In Orlando, the power went out and it was restored. It is something that happens, and there are different configurations of lanes so, you don't always have a chain of custody between when you assess the biometric and—

Ms. LOFGREN. What they have right now—and we looked at it—is the biometrics. It prints out a receipt. I don't want to get into the technology, that is a whole different issue, I just want to get into the positive ID and identity questions.

You identify this person, you get a receipt, there is a picture of the person on the right, and they give that with—there has never been, that I am aware of, a proposal not to put your computer through the X-ray machine or anything like that. It is a positive ID. I mean, how—your fishing license doesn't really tell you anything compared to a positive ID, does it?

Mr. HAWLEY. It is a matter of additional security, of having another credential with a picture on it.

Ms. LOFGREN. The thing that bothers me, if I may, is, the people that have not been back-grounded, people who just show up off the street in a line, have to show less ID than the people who have paid a fee, given their biometrics, had their whole history checked against whatever watch list the government wants. That seems ridiculous.

Mr. HAWLEY. Well, I draw your attention to Glasgow, Scotland, where those doctors would have cleared the watch list test—

Ms. LOFGREN. Standing on—without any background in Washington.

Mr. HAWLEY. It just makes the point that knowing that somebody's biometric is the same as the person traveling does not give you a risk basis on knowing whether that person—

Ms. LOFGREN. That leads me to a bigger question, because in the briefing we had—I was not able to go, but I had a staffer with a security clearance who did, who advises that we were told there were five or six watch lists that were checked.

I wasn't there. But even so, we spent a lot of money on these watch lists. We are using it for passenger lists from Europe. We are running—I mean, my husband can't get his boarding pass from the kiosk because there is probably some IRA terrorist with the same name.

We are saying that list matters except when it is being used by the Registered Travelers?

Mr. HAWLEY. No. I think does matter, but it is not sufficient alone. That is why we have to have the other layers. And that is why the concern of "clean skinned" terrorists; and the National Intelligence Estimate was very clear in saying "clean skinned" terrorists are a problem, and we have to account for that in our security.

Ms. LOFGREN. I think you are a nice person, but what you are saying does not logically add up.

If the bottom line is that the people who have had their biometrics and personal history checked, they were checked for fraudulent documents, have to give more ID than somebody who wanders in off the street, there is something wrong with this picture.

Mr. HAWLEY. The key point is having the background check, and under the Registered Travel program there is no background check; it is a check against the watch list. And that is a very big difference.

I think the logic that was articulated earlier makes sense. If there is a background check, you could give security benefit, but today it is simply, has the government identified you as a terrorist? If yes, then obviously we go pick you up. If you are not identified as a terrorist, then, you know—

Ms. LOFGREN. My time has expired, but I think—this doesn't add up to me. And I would like to note also that this whole program

is paid for by the participants, the passengers, they pay a fee. It is not the taxpayers paying.

I thought it was important to note that, and I yield back since my time has expired.

Ms. JACKSON LEE. Thank the gentlelady. Her time has expired.

I consent to yield myself for 1-1/2 minutes.

Quickly, Mr. Hawley, we are going to bring up the other witnesses, but let me ask you, do you believe in this technology? Do you believe it is viable, it is workable, with, a view in your mind, improvements?

Mr. HAWLEY. The technology is workable, and when it performs in a machine at the checkpoint, we will welcome it.

Ms. JACKSON LEE. As these standards have been issued, as my colleagues have indicated, and this company—the companies or the research—is going to move to utilize these standards, would that make it a better tool in Homeland Security?

Mr. HAWLEY. Yes, ma'am.

Ms. JACKSON LEE. Is your concern that—I understand what you are saying is that you don't consider the watch list as sufficient vetting and, therefore, that does not equate to you as a sufficient background check? Is that my understanding?

Mr. HAWLEY. To change the security regime.

Ms. JACKSON LEE. Because a person not on a watch list, such as doctors would not be, if you will, caught on that watch list?

Mr. HAWLEY. That is correct.

Ms. JACKSON LEE. So, therefore, we have a meeting of the minds, I believe, have an opportunity with TSA to look at an improved background check scheme, if you will, to look at the improved technology and have you leave the table with the idea that we should not ignore this kind of technology that may be not only good for convenience, which I would like to subrogate to security, but that it may work security-wise with all of the elements in place.

Mr. HAWLEY. Yes, ma'am.

Ms. JACKSON LEE. Let me thank the witness for his testimony. And I appreciate his service.

I look forward to working with you and ask the other witnesses to come before the committee.

Ms. LOFGREN. Madam Chairwoman, while the next witnesses are coming forward—

Ms. JACKSON LEE. The gentlewoman is recognized.

Ms. LOFGREN. Unanimous consent to place in the record the correspondence between myself, Mr. Thompson and the agency on this subject.

Ms. JACKSON LEE. Without objection.

We welcome the witnesses to the second panel and begin by introducing you and thanking you for your patience.

Our first witness will be Mr. Tom Conaway, Managing Partner, Homeland Security, Unisys Corporation. In this capacity, he spearheads efforts to position Unisys as an end-to-end services provider and plays a lead role in Unisys' homeland security strategy. Tom has responsibility for managing the Unisys engagement with the TSA, an unprecedented multiyear task order to build an advanced information technology infrastructure. Initially, it will help to se-

cure the safe transport of passengers and cargo throughout the United States.

Our second witness is Steve Brill, Chairman and CEO, CLEAR, Verified Identity Pass, Inc. Mr. Brill is the founder and CEO of Verified Identity Pass, Inc. and the creator of the CLEAR Registered Traveler Program. CLEAR, with over 53,000 members, is the largest privately run, registered traveler program operating at U.S. courts.

Our final witness is Mr. Bill Connors, Executive Director of the National Business Travel Association, NBTA.

We welcome you and we thank you. And in the spirit of full disclosure, Mr. Brill attended the law school of my spouse. And might I celebrate what a great law school it is? So let me.

Mr. BRILL. You and I went to college together.

Ms. JACKSON LEE. Might I ask the witnesses if you each will provide your statement in its entirety and summarize, we will acknowledge that will be accepted into the record. And we would greatly appreciate your provocative and abbreviated testimony so the members will be able to ask questions.

I am not sure when the next votes will be coming.

**STATEMENT OF TOM CONAWAY, MANAGING PARTNER,
HOMELAND SECURITY, UNISYS CORPORATION**

Mr. CONAWAY. Good afternoon, Chairwoman Jackson Lee, Ranking Member Lungren and the distinguished members of the subcommittee. I am Tom Conaway, Managing Partner for Homeland Security at Unisys.

In summary, Unisys has a long history of working technology solution programs for public and private sector customers, including several very large, biometrically based ID management programs around the world. Here at home we have been working for the Department of Homeland Security from the beginning, and especially the Transportation Security Administration, on programs such as US-VISIT, SBI.net, missing critical applications at CDPN and henceforth.

For the Transportation Security Administration, we were one of the two original contractors who worked on the pilot program. We ran three of the five airports that were used to test different technologies and techniques for putting people through the process. The things we learned during that pilot period laid the groundwork for what is being rolled out today. Case in point: At that time really there were no biometrically based programs in existence in the U.S.; there really wasn't any idea how society would respond to something like that.

We helped move that from the realm of science fiction to reality today, going from the pilot phase into the current pilot phase, because there still is a pilot phase, given that I think the idea was to do 20 airports.

Currently, we are now live and operational at the Reno/Tahoe Airport, so we are one of the two actual operating providers of the Registered Traveler. There have been some growing pains as this has rolled out. Some of those growing pains are similar to what would be seen at any roll-out for a new program, but there are some additional challenges that have to be faced, and you have

gone through several of them today. I won't reiterate that, but given that, under TSA's leadership we have formed a public-private partnership and look forward to working with TSA and Registered Traveler and their operability consortium to work through those and implement them.

Madam Chairwoman, that is a summary of my statement and I would be happy to answer any questions.

Ms. JACKSON LEE. Mr. Conaway, I think you will be called back as a witness over and over again. Thank you for your testimony. [The statement of Mr. Conaway follows:]

PREPARED STATEMENT OF THOMAS M. CONAWAY

Good afternoon Chairwoman Jackson-Lee, Ranking Member Lungren, and other distinguished Members of the Subcommittee. I am Tom Conaway, Managing Partner for Homeland Security at Unisys Corporation. We thank you for inviting Unisys to participate in this hearing focusing on the implementation of the Registered Traveler Program.

Unisys is a global corporation of 37,000 employees in over 100 countries providing information systems solutions and services to a wide range of private and public sector customers. We are a publicly-traded corporation with annual revenues in excess of \$5B. We are a U.S. company with our headquarters in Bluebell, Pennsylvania. And we have a long and proud history of serving our federal government.

Around the world and here at home, Unisys is a leading provider of integrated security solutions—many of which incorporate advanced biometric and identity management technologies. For example, we delivered a system to the Chilean Border Police that screens individuals arriving at airports against Interpol watch-lists based on facial recognition. We delivered a national identification card for Malaysia that employs fingerprint identification. Recently, we have been tasked by Australia, New Zealand, and Canada to test a variety of technologies to control land, sea, and air borders.

Here at home, we have worked on a number of initiatives aimed at securing our homeland and have worked directly with the Department of Homeland Security since its creation. As examples, we designed, developed and implemented in record time the initial exit-tracking capability for the US VISIT program. At Customs and Border Protection, we support the development and maintenance of mission critical software applications like the Free and Secure Trade System and the Automated Targeting System. We are also working on the Secure Border Initiative as a member of the Boeing-led SBInet team. At the Transportation Security Administration, Unisys currently provides a wide range of information technology operations and maintenance support. Additionally, we have also supported such programs as the Airport Access Control Pilot Projects and, of course, the Registered Traveler Program.

Unisys is proud to have worked with the TSA on Registered Traveler Program from the beginning. In June 2004, TSA selected Unisys to develop and operate three of the initial five pilot sites to demonstrate the utility of the Registered Traveler concept. At those sites, Unisys tested and analyzed various combinations of technology and techniques. The results gained from those tests supported the ultimate technology decisions TSA made for the program that is being deployed today.

One of the biggest unknowns at the time was the question of whether or not the traveling public would accept the program. The concept of using a biometric—other than a photograph—to verify the identity of an individual seemed more science fiction than reality. Even though there was initial skepticism, survey results of program participants indicated widespread acceptance and support of the concept. So much so, in fact, that TSA extended the program well beyond the originally planned performance period of ninety (90) days per airport.

As the TSA moved forward with the program, it became obvious that, even though it was popular with participants, it would not be economically feasible to implement a national roll-out using federal dollars. Therefore, a commercial model was created and piloted to demonstrate the viability of a different economic model that was based on subscription fees rather than a central federal budget.

The TSA took the lessons learned from these activities and used them to craft the Registered Program pilot phase that is being deployed today. Under TSA's leadership, what has emerged is a public-private partnership with TSA retaining overall program oversight and the Registered Traveler Interoperability Consortium (RTIC) providing a central voice for airport and industry participation. Working together,

this partnership has resulted in a technical interoperability specification that requires all certified RT vendors to produce and issue credentials and readers that allow program participants to travel seamlessly between participating airports, regardless of the source of enrollment. This is similar to you being able to use your ATM card in any teller machine, regardless of the brand of your home bank.

Much progress has been made and today the RT program is operating in at least six airports, with more on the way. The Unisys offering, rtGO, has been operational at the Reno-Tahoe airport since the end of May, and our customers are anxious to see the program expand.

Yet, with all this progress, several challenges remain. Some of these are routine "growing pains" associated with the roll-out of any new program. Others will require more thought and effort to resolve. This latter category includes the concepts such as: an interoperability transfer fee to be paid between the RT provider companies; the introduction of new screening technologies into the passenger screening lane; and the provision of benefits—such as not having to remove a laptop from a carry-on, or being able to leave shoes and jacket on—from the TSA.

Even though these challenges exist, the history of the program has shown that we will work through them. To that end, Unisys looks forward to working with the TSA, the RTIC, and the other RT providers to make this public-private partnership a reality.

Ms. JACKSON LEE. Mr. Brill, welcome.

**STATEMENT OF STEVEN BRILL, CHAIRMAN AND CHIEF
EXECUTIVE OFFICER, CLEAR/VERIFIED IDENTITY PASS, INC.**

Mr. BRILL. I am glad to be here. I represent CLEAR, which operates 11 of the 12 Registered Traveler airports.

Our airports and our 53,000 members love RT, an astounding 90 percent of those who joined in Orlando, where we started 2 years ago, have renewed their annual \$99 subscriptions. We process people faster; it takes them half a minute to 4 minutes to go through security. Yet, in Orlando, we process 15 percent of the people using 6 percent of the lanes.

You know what? I will take this statement and put it over here because it doesn't matter.

What matters is what you have pinpointed, Madam Chairwoman, and that is security, that is the first thing that matters. I think Kip Hawley is a terrific public servant. I took a lot of grief from journalists a while back from writing very good things about TSA and about Mr. Hawley, but he is dead wrong about this program. This program is a security program.

Nothing Mr. Connors says, although I respect about how it provides more convenience for businessmen, more efficiency in the business world, none of that matters if it is not a security program.

Mr. BRILL. This is a security program, and allow me to explain it. First of all, we have gone through thousands of pages of audits, self-audits, TSA audits for every airport where we have launched. We have had to adhere to super encryption systems, we have had to have two attendants enroll each member, a requirement that DHS does not even use for the credentialing of its own employees.

After all of those security hoops, which cost us millions of dollars, what do we have for it? We have nothing in the way of security benefits. But, you know what, we are not asking for anything. What we are asking for is what Congressman Norton said, is that in return for going through all those security hoops, for providing better biometric identification, better background screening than is done for freight workers, who Mr. Markey is told all the time are so well background screened that you don't need a real secure freight program.

In return for going through better screening than airport workers go through, than freight workers go through, than the RTIP program does, we get no security benefits. But no one has asked for it. What we have asked for is that the equipment that we have paid for, that we have developed with GE and other equipment that other competitors develop, that that equipment be tested quickly.

In February of 2006, I sat with Mr. Hawley and someone from GE and we were told that equipment would be put on a fast track. Now there are some of you who think that for TSA that is a fast track. I wrote a book about an organization that was launched in 2002 where fast track really was a fast track, where people had a can-do attitude and they got things done.

They have not done that with Registered Traveler. I think there is a reason for this. The office that oversees Registered Traveler is the office that oversees the RTIP program and the Secure Flight Program. There is a difference. We are a private sector program. We are not contractors. My friend Mr. Conaway here obviously has to be nice to TSA, he has multiple contracts with them. I don't.

I am not here seeking money from the government, I am here asking the government to get out of the way, to do its security job to supervise a security program so that we can make this country more secure and, yes, so that our business will be profitable.

We estimate and we know that if this program rolls out 30 to 50 percent of the people moving through a busy airport on a weekday morning will be pre-screened, will have their biometrics taken, will be screened, will be going through equipment that will test their shoes for explosives and test their fingers for residue of explosives at no cost to the taxpayer, and we think taking 30 to 50 percent of the hay out of the haystack is a security program.

We think that the bureaucracy at TSA has preferred to dismiss it and say it is not a security program, it is just about convenience. You use the convenience to lure people in so that we have a business and so that TSA suddenly is screening 30 to 50 percent of the people with real biometric credentialing, with better equipment. I think that is a security program.

I am not in the business of providing more convenient parking for people, or anything else. I had a vision that we could start a voluntary credentialing industry. The President put a white paper out almost 2 years ago today, actually 2 years ago—5 years ago yesterday asking for the private sector to innovate and join the fight for homeland security. That is what this voluntary credentialing industry is about. It is not about providing convenience, it is about offering convenience in return for getting and maximizing security.

We need your help to bring that promise home and, yes, it is true that a 12 to 18-year old who is a member——

[The statement of Mr. Brill follows:]

PREPARED STATEMENT OF STEVEN BRILL

Madame Chairwoman, members of the Committee, I'm delighted to be here today to represent Clear, which now operates the Registered Traveler program, or is about to, in 11 of the 12 RT airports. We currently operate Registered Traveler programs in Orlando, San Jose, Cincinnati, Indianapolis, Newark and John F. Kennedy in New York.

By the Fall, we will be operating programs in San Francisco, LaGuardia (New York), Albany (New York), Little Rock, and Westchester.

And Dulles, Reagan, Denver, Atlanta, and Miami are among the major domestic airports which have announced plans to launch Registered Traveler (RT) this year.

The airlines initially had a wait-and-see attitude. But we now have sponsorship and marketing partnerships with British Airways, Air France, Virgin Atlantic and—our first domestic air carrier—AirTran Airways, with other domestic and international carriers about to join.

Word of the advantages of this common sense program has even spread abroad. We are working with governments, airports, and airlines in Canada, the United Kingdom and Europe to launch Registered Traveler.

The logic of the program and the process is simple: If people volunteer to provide some biographical information about themselves so they can be screened in advance, the availability of cost-efficient biometric technology now enables them to be issued a card that only they can use in order to expedite their process through security. Moreover, the membership fees they pay should also enable their Registered Traveler service provider to deploy enhanced security equipment at the RT lanes which should aid in allowing members an expedited security process. The prime current example is a shoe scanner that we have co-invented and developed with GE that scans shoes so that our members will not have to remove them as they pass through the TSA checkpoint.

But this is both a good news and a bad news story, and we need your help to correct the bad news.

The Good News—More Than 50,000 Members With Millions on the Way, Better Security, Better Equipment, Faster Lanes for All, and 30%-50% of the "Hay" Removed From the Haystack

Our 53,000 members love the program. They appreciate that the technology works and that it takes them a half minute to four minutes to get through any lane at any of our airports. And they appreciate our trailblazing privacy policies, which include independent public privacy audits of our system and what I think is the nation's first identity theft warranty. More than 90% of those who joined in Orlando—where we started two years ago last week—have renewed their annual 99 dollar subscriptions. In my former life as a magazine editor and publisher, a 90% renewal rate would have been heaven.

At the pace we are now taking enrollments, and with those renewal rates, we could get to four million members domestically within three years, if—and this is the big “if,” as I will explain—the bureaucracy of the Transportation Security Administration (TSA) stops trying, for reasons I can only speculate about, to stunt the program.

Most important, RT improves aviation security. The thousands of road warriors who go through our lanes every day are the only people who have been pre-screened by TSA and whose identities are absolutely assured by their use of biometric cards at our verification kiosks. And our estimate is that once RT is allowed to reach its potential and is rolled out over the next 18 to 24 months, 30—50% of the travelers moving through a big airport on a weekday morning will be pre-screened, biometrically-verified RT members. That's because RT members travel so frequently that they make up an enormously disproportionate share of the flying population, and it's because we project 50,000 to 200,000 members at each airport where we launch. That takes a lot of hay out of TSA's proverbial security haystack—all at zero cost to the taxpayer.

Think about that: a voluntary private sector program that achieves a third to half of one of TSA's basic missions at no taxpayer cost.

Airports with RT are also more efficient for all travelers. In Orlando, we regularly process 10–15% of the passengers moving through the airport using just six percent of the TSA checkpoint lanes. That means that not only does Clear give its members a fast, predictable experience when they arrive at airport security, but it also means that the lines for everyone else are shorter because our lanes process more than their share of travelers.

The analogy here is electronic tolling. As long as the electronic lanes and non-electronic lanes are apportioned correctly, *everyone* now goes over the Triboro Bridge and the Golden Gate Bridge faster than before electronic tolling was invented.

That's why every airport that has implemented the program loves it. And our customers love it so much that we're using quotes from them in a new national advertising campaign.

All of this would seem to be a good deal for TSA, in addition to air travelers and airports. And the deal gets better. As you know, because you have had an opportunity to see it demonstrated, we have financed new technology at the RT lanes that screens shoes for explosives as well as dangerous metal and that even tests for

traces of explosive residue on people's fingers, thereby making it possible for them to leave on their outer garments. If TSA allows this innovative technology to be deployed at our lanes, TSA would then get to see the technology working in the best possible testing environment—where travelers have already been vetted—and then decide whether to buy it for all lanes. The private sector will have created the market for the technology and paid the development costs as well. We think that's a good deal for TSA and the country.

The Bad News—TSA's Undermining of the Program

Yet, despite these benefits—voluntary pre-screening and identity verification, free development of technology, faster lanes—TSA has not been treating RT like a good deal. Rather the agency has allowed the program to happen grudgingly, behind schedule, and only then because, frankly, you in the Congress and we as entrepreneurs have pushed it.

TSA Administrator Hawley and Deputy DHS Secretary Michael Jackson—both of whom I have publicly praised for their roles in getting TSA up and running so quickly in 2002—have supported RT rhetorically, and Secretary Chertoff has made intelligent risk management a key mission of DHS. But, for whatever reason, TSA and DHS have not allowed RT to become what it can and should become. To the contrary, it seems that at almost every turn decisions that threaten to undermine RT have been made by the TSA Threat Assessment and Credentialing Office. That's the office also responsible for TWIC and Secure Flight. Perhaps the folks in charge there don't want to see a private sector program flourish while those government programs remain unfulfilled.

To give you the big picture, TSA now requires that we:

- *Write and submit separate System Security Plans totaling 317 pages per airport;*
- *Prepare and submit separate 305-page self-assessments of how we comply with hundreds of pages of TSA standards and specifications;*
- *Complete an Independent Pre-Implementation Audit of Compliance from a Big-Four firm with relevant American Institute of Certified Public Accountants standards for each airport that costs over \$200,000 and audits approximately 1,000 control points;*
- *Adhere to hyper-secure specifications for card encryption and data transmission;*
- *And adhere to the unprecedented (in any similar federal identity credentialing program, including the credential of DHS employees) requirement of not one but two security-screened attendants to complete each enrollment in order to protect against collusion.*

It all adds up to an enrollment, card encryption and security system that is more stringent not only than that used for any airport workers—who typically don't even have biometric cards—but more stringent than that used for the identity documents issued to members of the Pentagon or Department of Homeland Security.

All of that security makes sense—and we applaud it—as a condition of RT members getting some relief from the standard airport security process. That certainly was Congress's intent—because that's smart risk management. But here's the catch: Our members now enjoy an expedited process *only* because of the concierges we use at our lanes to help them place their necessary items into the bins and then retrieve them after the screening is completed. That has speeded throughputs by 30%. But, as of today, RT members get nothing in the way of an amended security process in return for the security threat assessment, biometric verification, and thousands of man hours and audit pages and dollars of security hoops that we jump through.

In fact, the opposite is true.

The "Double ID" Rule

Beginning last fall, TSA suddenly required that RT members using the RT line show a picture ID *and* their RT card right before entering the line. These are the same RT cards that, when put into the RT kiosk, will use the traveler's fingerprint or iris scan to biometrically match the user to the data embedded in the card. That's right. RT members are the only travelers who must present TWO forms of identification. When Mr. Hawley testifies, he may give you one or more of the many different explanations for this that he has given us over the past year. I would take the time here to rebut all of them, but the explanations, for what is obviously a mistaken directive that no one now wants to admit was a simple mistake, seem to change every week.

So, let me just address two of TSA's purported explanations, including their most recent one. In letters last month, Mr. Hawley maintained that a photo ID must be checked to enter the RT line because the configuration of the RT verification kiosk and the TSA security checkpoint at some airports could "result in lack of control over ingress to both screening and the secure area." TSA completely misses the

mark. At every airport that features the RT program, the RT service provider and airport work hand-in-hand with the TSA Federal Security Director (whose approval is required) to satisfy the FSD that security and access control is in no way compromised as a result of the configuration of the RT verification lane. That is the appropriate and, indeed, the only way to ensure “control over ingress.”

By contrast, requiring that an RT member show a photo ID to enter the RT line (where s/he is then immediately biometrically verified) has absolutely nothing to do with controlling access to the area *between* the RT verification kiosk and the TSA screening checkpoint. This is simply apples and oranges. Moreover, this ignores the fact that our kiosk issues a receipt with the member's digital photo printed on it, which the TSA personnel can inspect at the entrance to the metal detector. That photo is produced when the member's biometric is presented—which makes it far more secure than some fishing license that non-RT members can present back at the entrance to the lane. This also ignores the fact that Mr. Hawley supposedly empowered local Federal Security Directors to approve all RT operations plans at each airport, and none raised this line of site issue (though they might now, given that the boss has conjured it up). Put simply, this argument is plainly absurd.

And, earlier this year, TSA explained that our members had to present a photo ID in addition to the RT card, because our RT verification kiosks wouldn't work if there were a power outage in the airport. Of course, if there were a power outage in the airport, in all likelihood *nobody* would be going through the RT line or the TSA security checkpoint, because TSA's magnetometers and x-ray machines wouldn't be working, so there would be no opportunity for our members to show their photo IDs to anyone. In short, it's another TSA explanation that makes no sense.

Pilot projects are supposed to be for research and testing. Our Orlando program, started two years ago, began as a pilot project. During that time, in which 300,000 members passed through our lanes, there was not a single incident in which the fact that our members did not have to present an additional photo ID ever caused a problem. Not one in 300,000.

The result of the implementation of the double ID rule has been predictable and unfortunate. Members have called and written Clear with complaints about the obvious illogic of this new rule, which requires them to present *more* in the way of identification credentials than other travelers. Clear has been at a loss to answer these complaints, because there really is no answer. To some customers, whose emails I read and whose calls I take every day, this makes the program, or TSA, or both a laughingstock. I really have no good answer for them.

In response, TSA has informed Clear that it will consider a solution in which photographs appear on the RT cards. As an initial matter, Clear questions the wisdom of this solution. It is just not smart security. One of the advantages of a biometric card is that security personnel become trained to “trust” a biometric match only. If a photograph is added to the card, it increases the possibility that a person for whom RT privileges have been revoked (based on a new assessment of the person's threat risk, for example) will nonetheless be able to convince security personnel to let them through by blaming the negative results of the biometric comparison on some sort of equipment defect. In any event, TSA has stated that it will not even *consider* the alternative of a photo appearing on the RT card unless *all* members of the industry unanimously agree to make it the standard for all RT cards, thereby giving our competitors—who are lagging behind us—a way to stop our progress while they catch up.

That is an abdication of TSA's regulatory role. TSA did not ask for industry unanimity when it unilaterally imposed the rule that requires two attendants for every enrollment. Why now, except to stiff arm this program? If TSA determines that placing photographs on RT cards is the proper solution, because it is better security, TSA should be the one to make that decision; and if it does, Clear will abide by it. But Clear's compliance with the rules should not be subject to the unilateral veto power of every other vendor—especially those that have expressed tentative interest by declaring themselves part of the “industry group” yet are not serious enough to commit significant resources to enrolling participants or operating lanes at airports. TSA should dispense with the photo identification requirement for RT participants or promptly announce that a photograph on the RT card will satisfy such a requirement.

None of TSA's explanations for the double ID requirement makes sense to any TSA security official I have ever spoken with outside the Credentialing office. I should add that when I first raised this issue with Mr. Hawley, he, too, said it seemed ridiculous and would look into it. But in a pattern that has now been often repeated, when Mr. Hawley consults his staff about RT, his mind always seems to change.

The Saga of The Shoe Scanner—or How Not To Encourage Private Sector Investment in Better Security

My second specific has to do with the shoe scanner I mentioned earlier.

In February of 2006, TSA invited us and General Electric, with whom we co-invented this enhanced RT security kiosk and which manufactures it, to let TSA test it for use at our lanes—and at the lanes of any of our competitors, to whom GE is also committed to supplying it. In return, RT members would not have to remove shoes once the technology was installed. We were told it would be put on a “fast track.” Then the Transportation Security Lab refused to accept it for testing. That standoff lasted until May 2006, and only ended after Mr. Hawley made multiple requests that the lab test it.

Testing then proceeded there, and then on the ground at our lanes in Orlando. In November 2006, after TSA had extensively tested the equipment, TSA provided what appeared to be exactly the clear path for the implementation of these kinds of industry-funded innovations that is necessary for this type of public-private partnership: Mr. Hawley told Clear that once his Chief Technology Officer (CTO) had briefed the relevant local Federal Security Director (FSD) on the benefits of the shoe scanner, and once the FSD agreed to implement the scanner, it would be implemented at that FSD’s airport.

Thus, in December 2006 conference calls with the CTO and the FSDs, the implementation was scheduled for January 2007. And in December 2006, TSA told the Wall Street Journal that the shoe scanner was approved for deployment and that people who went through the scan and passed the test and got a receipt—with their digital photograph on it—would then pass through without removing shoes. In a conference call with our team and local TSA officials in Orlando, the CTO confirmed that the equipment had tested well and was approved.

But three weeks later, on the eve of our national roll out and with no explanation, TSA rescinded this decision, although they allowed the shoe scanner to stay on in Orlando. The sole explanation we got was that a new CTO wanted to conduct a quick review of the prior testing.

In February of 2007 the RT program director told me in an email that the review and some new testing that had to be done would be finished by February 22 and that deployment would likely follow soon thereafter. It turned out, however, that no re-testing was being done at all, or at least that is what we are now being told.

It’s now July and as of today TSA is still not re-testing the equipment. That’s 15 months since it was put on the “fast track” by TSA. It would not surprise me if when he testifies today Mr. Hawley announces, finally, that the equipment is being tested again. I guess that’s why Congressional oversight is so important. But that will only raise more questions: What is the time line for the tests? What is the standard going to be? We and GE believe, and common sense dictates, that the standard ought to be not whether the shoe scanner can detect any molecule of any potentially dangerous element but whether it provides the same or better protection than that provided by putting a shoe through an X-Ray. Mr. Hawley has said that will be the standard, but I’m skeptical as to what the bureaucrats will do.

Interestingly, last month, TSA finally proposed a Memorandum of Understanding with GE to govern the testing of the new equipment, but then refused to agree to any meaningful terms. By way of example, TSA refused to provide any timeline for its testing and refused even to include a watered-down commitment that, if the new equipment satisfied *all* of the standards established by TSA, TSA staff would make a *non-binding* recommendation to the TSA Administrator that he allow the new equipment to be deployed with relevant security benefits.

The loss of public credibility and industry credibility has been incalculable. And incredibly, TSA has now been telling those in Congress or the press who inquire that there were “problems” with the GE equipment, an explanation that contradicts their own announcement to the press last December, contradicts everything GE has been told, completely contradicts the TSA email of February, 2007, and is just plain unfair to GE. How would they know about problems if they have not been testing it?

Things have now reached to the point where GE has formally notified us that they are about to cancel this project because neither we nor they can justify the investments in it, and GE, as a large public company, can’t keep spending money based on hope the way I can.

I am not comfortable saying all of this about TSA. Quite the contrary. As a journalist writing a column for Newsweek while I was writing my book, and then after my book came out, I was criticized by lots of colleagues for praising the people who launched TSA in the first year—including Mr. Hawley and Deputy Secretary Jackson. But I think I was right: they did do a great job getting TSA up and running and taking over the lanes on time. The question is what has happened since to an

agency that, when I was watching it, had no bureaucracy but instead had manically-dedicated “Go-Teams” run by Mr. Hawley. Teams that stood at meetings because the furniture hadn’t yet been purchased—and then went out to Staples to purchase it themselves when the paperwork to buy it got bogged down.

In one passage of the book, in describing how dedicated and unbureaucratic the TSA pioneers were, I wrote: “TSA-time was something akin to dog years only more so: in terms of how fast they had to move, a day is like a month and a month is like a year.” Although I still have no doubts about Mr. Hawley’s dedication, I keep thinking of that paragraph when I think about the continuing saga of the GE shoe scanner. And I know that the Go-Teams would have laughed that Double ID requirement right out of their makeshift conference room.

I also know that one of the first things Mr. Hawley does every day is go over current intelligence that provides a fresh reminder that there really are terrorists out there trying every day to kill us, and that some still want to use our aviation system to do so. I do not doubt his sincerity or underestimate the burden that he and all of his colleagues at TSA face. I just happen to believe that Registered Traveler and voluntary credentialing can be a significant part of the solution and that this program is consistent with—indeed the embodiment of—the intelligent risk management that Secretary Chertoff has declared is a core element of DHS’s mission.

The “Selectee” Override—Now You See It, Now You Don’t

My third specific has to do with a key feature of the Orlando pilot program that is no more. During the Orlando pilot, TSA authorized a participant’s RT status to exempt them from automated selection for secondary screening. (Of course, TSA retained the right to select any traveler randomly at any time for secondary screening.) The override was logical because the perpetual and real-time vetting provided for in the TSA-issued RT specifications, and to which registered travelers are subject, screens out the very people for whom this “selectee” status is designed. The automated selection criteria are based on generalizations about passenger risk that do not apply to the subset of travelers who have been pre-screened during the enrollment process. Excluding RT participants from this automatic selectee status allows TSA to focus on a smaller group of potentially risky travelers. TSA has now eliminated this common-sense feature.

TSA has told Clear informally that it has done away with the override because, for example, it limits the ability to designate all passengers on a selected high-risk flight as selectees subject to secondary screening. However, there is a much less blunt instrument which would address this concern while preserving the legitimate time-saving feature of the override. If TSA needed to designate all passengers (including any registered travelers) on a designated high-risk flight as selectees, the Federal Security Director at the originating airport could simply instruct the relevant RT service provider to provide *no* overrides during the time period that passengers for the designated flight are passing through the RT line; that way, all selectees passing through the RT line (including those on the designated flight) would be subject to secondary screening.

Clear *does not* propose eliminating random selection of RT participants for secondary screening. I agree that all security regimes must have an element of randomness. TSA should continue to subject RT members to occasional random secondary screening, while allowing any selectee status governed by certain imprecise data-related factors to be overridden more often than not at the discretion of the Federal Security Director through the use of an RT stamp—as was done in Orlando. Again, the issue is whether RT is truly going to become a risk management tool.

Help for Secure Flight, US-VISIT Rebuffed

Yes, we are a private company that will profit from our success. We don’t apologize for that any more than we seek sympathy for the risks we take in investing in a new industry and in trying to persuade customers to join, one by one. But our success offers more than the usual side benefits for our country. Unfortunately, TSA has stiff-armed those side benefits, too, again perhaps because it is a private sector program.

True, some of these offers would require adjustments to current program processes, but rather than welcome them or at least welcome the chance to explore them, TSA just says no.

We have, for example, offered to solve the predicament of people who are wrongly on selectee or no-fly lists—by giving them RT cards for free. RT solves this problem because, in order to enroll in RT, so-called “false positive” travelers (like all applicants) must present proof of the distinguishing characteristics that separate them from their No Fly namesakes, as well as biometrics that confirm their RT identities. Thus, the individual who does not belong on the No Fly list *would* get an RT card while the one who belongs on the list would not.

As a public service, Clear has offered to enroll *at no cost* all adjudicated false positives who are referred (at their request) to Clear; thus, they would not have to pay for their bad luck. TSA could then allow these registered travelers to proceed directly through the RT lane (at participating airports), where they would have to present their biometrically-based RT cards for verification. TSA would know that these registered travelers had already been cleared by TSA. As a result, false positive travelers who enroll in RT—again, at no cost—would be able to avoid the perpetual and terribly time-consuming process of establishing their innocence every time they fly. (As the RT program expands to more and more airports, the false positive travelers would get greater and greater benefit from this feature.)

TSA has ignored this offer, even though it would eliminate—at all participating airports—what I know is one of the most frustrating case work issues your offices deal with every day, as you try to help constituents who have the bad luck of having the wrong name.

We are already offering free cards to members of the military, and we are offering a discount of one free month to any government employee. But we've offered a much larger discount *if* TSA will recognize the screening that so many government workers have already gone through.

For example, we've asked that the threat assessments conducted by the FBI and Secret Service of their own agents be recognized by TSA, so that those agents can get cards for far less money. Even DHS headquarters employees have inquired if they can get a card at a reduced cost because they have already been screened—by DHS. Months ago, TSA gave the quintessential bureaucratic response to the question of whether the RT program will recognize the screening that many government employees have already gone through: "TSA is examining this possibility." But TSA also said that even if they eventually stop studying it and actually do it, they won't under any circumstance waive their TSA screening fee of \$28.00. That's totally baffling.

We have also offered to make our kiosks available for conducting the verification services for US-VISIT, a process that DHS now wants to make the airlines hire people to conduct with additional government-financed kiosks. That offer, too, has been ignored.

Finally, as TSA continues to struggle mightily to roll out Secure Flight, consider that RT can do 30–50% of Secure Flight's work—at no cost to TSA.

This is because registered travelers fly so often (an average of 40 times a year, according to the Orlando surveys) that they make up a dramatically disproportionate share of the flying public on any given business day. A registered traveler need not be subject to a Secure Flight search at all, because registered travelers will have been cleared in advance (and on an ongoing basis) through a TSA security threat assessment. Indeed, the RT background check is substantially superior to the likely Secure Flight background check, because only the RT background check will be supported by identity verification—first, at enrollment with a biometric and with scannable forms of tightly-defined forms of identification, and then again with a biometric whenever a registered traveler flies.

By having RT members tell the air carrier when making a reservation that they are RT members, their boarding passes could require that they pass only through an RT lane at the airport—where their identities would be verified biometrically. As a result, based on Clear's projections that in a full-fledged national program registered travelers will make up 30 to 50 per cent of all travelers moving through an airport on a busy weekday morning, TSA's daily Secure Flight searching burden could be reduced by as many as 1.25 million of the Secure Flight's total projected 2.5 million name-matching searches per day. RT's relief of Secure Flight can begin immediately (and grow) with each expansion of RT to a new location. And, again, those 1.25 million travelers would be going through a more secure process than Secure Flight is expected to offer. TSA has ignored this offer.

An Issue of Common Sense

Almost exactly five years ago this afternoon, President Bush promised in his first White House White Paper on "Securing the Homeland," that "The Department of Homeland Security will ensure appropriate testing and piloting of new technologies."

That promise was separated out in a box entitled "National Vision."

Certainly, enough time has passed for this modest goal to have been met, particularly when the technology to be tested is going to be financed by the private sector and will help secure our homeland. We hired no lobbyists to walk the halls of Congress looking for an appropriation. Instead, we invested our own private funds in new technology, sent the equipment to TSA for testing, and begged the government to let us deploy it at our expense.

If you sense frustration, you're right.

I got the idea for a voluntary, private sector credentialing industry because as a reporter writing a book about the aftermath of September 11, I read carefully, and was moved by, that White Paper, in which the President called on private companies to become “a key source of new ideas and innovative technologies that will enable us to triumph over the terrorist threat.”

My notion was that this new industry should be strictly regulated by the government, and that the government needed to do the screening; but I was also convinced that only the private sector could provide—through a competitive marketplace—the privacy assurances, the customer service, the cost-efficiency, and the technology innovation necessary for this industry to succeed. I still believe that. And that belief is validated by the fact that when TSA launched its own pilot programs in 2004, which they ended in 2005, they spent \$1,500 per card for a program that offered little customer service.

This is not a partisan issue, and it hasn't been one in this Committee. Enhancing security by providing secure biometric identification and pre-screening to 30–50% of the travelers moving through the nation's airports on a weekday morning at zero cost to the taxpayers, while allowing hard-working road warriors to spend an extra half hour at home and then get through the airport security line at 6 or 7 in the morning with less hassle, is not a Republican or Democratic epiphany. It is a matter of simple common sense—and national security, given how much hay it takes out of TSA's security haystack and how much in the way of new time-saving and security-enhancing technology it could provide.

This is why Registered Traveler has enjoyed strong support from both sides of the aisle in this Committee and across Capitol Hill.

Getting to Two Million Members in 2008, Four Million by 2010

Everyone engaged in the creation of the RT program now needs your help to facilitate the testing and approval of new technology in order to provide benefits in the checkpoint screening process—such as being allowed to you're your shoes on, or in the case of our explosive trace device, not having remove your outer garments.

Even if those benefits do not materialize in the short term, we may get to 200,000 members by year end. But with those benefits and the elimination of the double ID requirement, I am confident we will get beyond 500,000 by year end, to two million by the end of next year, and to four million by the end of 2010. We continue to gain members and offer a real service because the benefits we provide help speed the process at the lane. But allowing the deployment of the enhanced security equipment would propel the appeal of RT much further—while also providing, we believe, better security equipment at these lanes.

And, obviously, we need you to help get rid of the double ID requirement, which we believe has already lowered our renewal rate from the mid-90's to 90 percent, as some members vent their well-deserved frustration over a requirement that is so nonsensical that to some it makes us and the entire program a laughingstock.

The Saga of the Twelve Year Old—Two IDs at the RT line; No ID's at the Regular Line

I'll conclude with one more, almost comic, story that illustrates the state of play. Under TSA regulation, children between the ages of 12 and 18 can apply for and get RT cards. Also, as you know, people under 18 do not have to show ANY form of identification at an airport. You probably know where this story is going.

Yes, TSA recently ruled that a 12 year old RT member must not only have his biometric RT card but must also carry his passport or produce some other form of government ID (which he is not likely to have with him, because few 12 year-olds carry one—because they don't drive) in order to get on our line. Yet he can get on any other line and complete the screening process without showing ID of any kind, and if he uses one of those lines there will be no opportunity to confirm his identity using the biometric data embedded in his RT card.

Please ask TSA to explain why that makes sense. Ask why that is good risk management. Please ask TSA to explain why the double ID requirement for any RT member makes any sense. Ask what the purpose is of the security vetting and biometric verification and those thousands of pages of documentation and audits and the millions of dollars worth of encryption technology and enrollment processing that surpasses that used for DHS's own headquarters employee cards. And please ask why TSA still has not re-tested the GE equipment and why TSA has refused even to sign a memorandum of understanding with GE that specifies the timelines for the testing and includes even a mention of the benefits RT participants and the rest of the traveling public might enjoy if the re-tests are successful.

Thank you again for this opportunity to appear before you—and for your support of this important risk management program.

Ms. JACKSON LEE. The gentleman's time has expired.

Thank you. Mr. Connors, you are recognized for 5 minutes.

**STATEMENT OF BILL CONNORS, EXECUTIVE DIRECTOR AND
COO, NATIONAL BUSINESS TRAVEL ASSOCIATION**

Mr. CONNORS. Thank you, Madam Chair and Ranking Member Lungren, and thank you, subcommittee members. I am the Executive Director and COO of the National Business Travel Association. We represent more than 3,000 major corporations and their travel managers, buyers and planners, and they represent some tens of millions of actual frequent business travelers. So I guess I am the panelist up here who actually represents the end users of this system.

And we do, I agree with Mr. Brill, we do believe this is a security program, not just a convenience program. But there is nothing wrong with a little convenience either.

NBTA is a strong proponent of the Registered Traveler Program and has been for several years. For the business traveler, time is money, and this program creates a much more predictable airport travel experience and takes some of the hassle out of the hassle factor.

It would enhance the experience while increasing security by allowing airport screeners to concentrate on unknowns rather than knowns. We believe the RT program can live up to the title of this hearing and manage risk and increase efficiency.

Throughout the public debate on RT, NBTA has consistently advocated seven key points. Number one, that it is voluntary in nature. Number two, that it is broadly available. Number three, that it is interoperable between airport and RT providers. Number four, that expedited screening is provided in a dedicated lane without slowing the other travelers. Number five, protection of participants' data is crucial. Number six, the public understands the actual benefits of the Registered Traveler Program. Number seven, it enhances the overall security of our aviation system.

In assessing these seven items NBTA believes progress is well underway on all of them. Four of these, voluntary participation, interoperability, enhanced security and protection of data, are all built into the RT business model. Others, like broad availability and the public understanding of the cost and benefit, are all works in progress. My written statement goes into that in more detail.

While our forecast for the RT program might be rosy, there are some areas of additional attention that may be warranted, and many of you have already discussed those, but one I would like to add, an increasing number of our travelers are traveling overseas in this global economy, and in recognition of this, the 2008 DHS appropriations bill include provisions to authorize an International Registered Traveler Program, and we hope the House and Senate conferees will support that provision as well.

Finally, we would like to remind everyone that RT is just one program within a broader layered security system and is a risk management concept supported by the 9/11 Commission and travel organizations like ours.

Madam Chair, thank you for this opportunity. We believe RT can be a program that will enhance travel security as well as our eco-

conomic security by promoting the healthy conduct of commerce in our global economy.

Thank you.

[The statement of Mr. Connors follows:]

PREPARED STATEMENT OF BILL CONNORS

Good morning Madame Chair and Members of the Subcommittee. My name is Bill Connors, and it is my honor to testify before you today on behalf of the membership of the National Business Travel Association (NBTA).

As the authoritative voice of the business travel community, NBTA represents more than 2,500 corporate travel managers and travel service providers who collectively manage and direct more than \$170 billion of expenditures within the business travel industry, primarily for Fortune 1000 companies.

NBTA Support for Registered Traveler

NBTA believes that Registered Traveler (RT) programs enable a more secure, faster, and more consistent screening process. This, in turn, enables the more than 6 million frequent business travelers to be more productive while enhancing the security of our nation.

As a result, NBTA has been a strong supporter of the RT concept since its inception. We have participated in the original DHS pilots at airports in Minneapolis, Boston and Washington, DC. In fact, I was a member of the RT pilot program here at Reagan National Airport.

Throughout the public policy debate on RT, NBTA has consistently advocated 6 key points which we believe are the keys to success:

- Voluntary participation (opt-in)
- Broad availability
- Interoperability between airports and between RT providers
- Demonstrably expedited screening provided in a designated lane without slowing other travelers
- Robust protection of data collected as part of Registered Traveler enrollment
- Public understanding of the benefits offered by Registered Traveler, the costs associated with participation, and the security check process

NBTA Assessment of Where we are Today

In assessing these six points today, NBTA believes progress is well underway on all of them.

Three of those—voluntary participation, interoperability and protection of data are all built in to the TSA RT business model.

Three others—broad availability, demonstrably expedited screening in a designated lane, and public understanding of the costs and benefits—are all works in progress. Let me go into each of these in a little more detail.

Broad Availability

One of the keys to having RT realize its potential to more predictably and securely move travelers through airports is having the program reach sufficient scale. That is, travelers to top airports should have access to RT programs on all legs of their trip. While there is some value in being able to use this program on even one part of a business trip, our members are keenly watching to see the program grow to all major airports, thereby adding predictability throughout more of a business trip.

Today, several airports are currently online with registered traveler programs

- JFK, with three terminals offering programs
- Cincinnati/Northern Kentucky International Airport
- Indianapolis International Airport
- San Jose International Airport
- Orlando International Airport
- Reno Tahoe International Airport
- Terminal B at Newark

Other airports are in the final stages of building out their RT programs, having already selected a vendor:

- San Francisco
- Albany
- Westchester County Airport
- LaGuardia
- Little Rock

Additionally, several airports are having RT services built now, or looking to acquire them, including

- Huntsville International Airport
- Los Angeles International
- O'Hare
- Denver
- Miami
- Washington Dulles
- Washington National

It's interesting to note that while we speak, the Washington DC area airports are considering bids from approved RT vendors to roll out the program here in our area, with Baltimore expected to follow suit soon thereafter.

Demonstrably Expedited Screening

When talking to business travelers about their reasons for seeking an RT card, one stands above all others—predictability in moving through the airport, curb to curb. They expect these designated security checkpoints to allow them to move more quickly and efficiently through the airport, bypassing the long lines often created by infrequent travelers who are unfamiliar with checkpoint security procedures. While many people believe that the so called “big three” security benefits of RT—keeping lap tops in bags, keeping coats on and keeping shoes on—are the keys to demonstrably expediting screening, we would add the following perspective. While these three items would surely speed business travelers through checkpoints, what our members have already adapted their flying habits to account for these procedures.

From the frequent business traveler perspective, the key to moving through checkpoints today is traveler behavior and familiarity—or lack thereof—on how to rapidly move through the TSA checkpoint. To the degree that RT lanes are used by frequent business travelers who know how to efficiently move through the checkpoint, that in and of itself is a benefit of the program.

Therefore, as RT vendors test and deploy new technologies that allow travelers to keep their laptops in their bags, and keep their shoes and jackets on, we hope that the new technology will not slow down the travel experience of our members moving through RT lanes today.

Public understanding of the costs and benefits

The last point NBTA would like to make is on the public understanding of the costs and benefits of the RT program. This is an area where both the RT vendors and the TSA leadership have a responsibility. In this vein, we have some recommendations for both sides on how they can be more effective.

On the private sector side, we feel confident that all of the vendors do a great job touting the benefits of their own programs—and that's to be expected. As vendors invest in security enhancing technology and use it to gain market share, we will be on the lookout for any confusion that might arise in the marketplace, particularly around the issue of interoperability of RT systems.

Our final issue in the area of public understanding is the role of the federal government. While this is a private sector program overseen by the government, the TSA has an important role to play in supporting the concept of RT. It is, we believe, perfectly aligned with the risk management philosophy espoused by the Administration and homeland security experts. However, we often hear inconsistent messages out of TSA—some wholeheartedly supporting the program, others casting doubt on the value of background checks performed, others focusing on the investments RT service providers will have to make in order to have customers realize security benefits.

These varied messages can create confusion among the public and make many of us in the private sector doubt TSA's commitment to the program. We certainly hope that TSA and DHS will soon consistently deliver strong public messages of support for RT, and save deliberations on program improvements for private conversations with stakeholders.

The Future of RT

While we believe the forecast for the growth of RT is quite rosy, there are several areas where NBTA believes additional attention is warranted.

Over the next 12 to 18 months, we expect the number of airports with RT programs to grow to most, if not all, of the top airports in the nation, thereby providing true value for business travelers. With such a critical mass of airports involved, we believe certified RT services providers will begin to more aggressively work with the employer community to expand opportunities to enroll in the program, perhaps by locating kiosks in corporate headquarters, hotels, convention centers and the like.

By taking steps like these to make enrollment more widespread, momentum can be built to encourage additional airports to contract with RT services providers.

Additionally, the government and private sector RT vendors should give strong consideration to enhancing efficiency at airport checkpoints by auto enrolling in the program segments of the population that are known to pose negligible security risks. Federal workers with security clearances, members of the Transportation Worker Identity Credential program, and enrollees in the U.S.-Canada NEXUS program—are good examples of such populations who should almost automatically be included in RT, given the security checks they have already undergone.

Third, we would like to note that an increasing percentage of a business traveler's time is spent visiting growing foreign markets. In recognition of this trend, the Senate passed version of H.R. 2368, the 2008 Department of Homeland Security Appropriations bill, included provisions by Senator Mel Martinez (R-FL) and Senator Susan Collins (R-ME) to authorize an International Registered Traveler (IRT) Program. Like the domestic program we have been discussing today, the IRT program would expedite the security checks for frequent international travelers traveling to the United States. We hope that all the House and Senate conferees will support this provision and include it in the DHS appropriations bill that is eventually sent to the President.

Finally, we would remind the committee that RT is one program within a layered security system governing our air transportation network. When deployed in conjunction with Secure Flight, the soon to be announced government effort to vet unknown travelers, RT is a key part of build both efficiency and security into our system. We certainly hope that TSA soon moves to deploy the long-delayed Secure Flight program and utilizes it effectively, from both security and privacy perspectives.

Madame Chair, thank you again for giving me the opportunity to come before you today and provide the views of the business travelers, corporate travel managers and travel service providers on the Registered Traveler program.

Ms. JACKSON LEE. Let me thank the witnesses on the second panel for their testimony. And I will remind each member that he or she will have 5 minutes to question the second panel. And I will begin by yielding myself 5 minutes.

When Mr. Hawley finished his testimony and answered my final question, as the representative for the Transportation Security Administration, he indicated that he was not opposed to the technology, that he was open to the technology, and that he was looking forward to the standards that were recently issued being applied to the technology in the coming months.

Mr. Brill, what is the time frame for compliance with the standards now that I understand have been issued by TSA?

Mr. BRILL. There is no time frame that has been issued. They have told General Electric 17 months later that they can come in—they can now bring this back to be retested. There is no schedule that I know of. General Electric asked them to put it in a simple memorandum of understanding language that said if this is tested, if it passes the test, you will recommend to the Administrator that this benefit be included. They wouldn't even agree to that.

Ms. JACKSON LEE. This is TSA staff?

Mr. BRILL. It is the staff that is the issue here. This program has been stiff-armed at every step.

Ms. JACKSON LEE. You didn't answer my question.

Mr. BRILL. The answer is there is none.

Ms. JACKSON LEE. There were standards issued that would improve the technology, to my understanding. Is that correct? That TSA indicated that they wanted to see the next step of technology as relates to explosive materials in the shoe?

Mr. BRILL. GE has been given standards by TSA as of yesterday, the day before.

Ms. JACKSON LEE. Is it my understanding GE is going to move forward?

Mr. BRILL. Exactly. As fast as they can.

Ms. JACKSON LEE. That is the answer. They are prepared to move forward on at least the representative requirements that TSA says they have to have. They are ready to move forward, the private sector.

Mr. BRILL. Correct.

Ms. JACKSON LEE. The difficulty, as we heard in the earlier panel, is the affirmation or the approval by TSA that this program will be implemented.

Mr. BRILL. Yes. And to break that down a little bit, once the standard is set and once the test is passed, which we saw happen in Orlando, Mr. Hawley assured me at that time that as long as the FSD, the local federal security director approved the implementation, everything would go forward, and then that didn't happen; it turned out there was another office and then another office that had to approve this.

If you sense skepticism in my voice it is because at every turn something else keeps coming up that is not about security, it is not about security. TSA is in charge of security, not us. It is not about security. And I think this office has never gotten over the fact that they started the pilot project that my friend Mr. Conaway ran, the government spent \$1,500 per card for the pilot projects to find out that the technology worked and then suddenly it became a private sector project for \$99.

Ms. JACKSON LEE. Why do you think Mr. Hawley is asking for an additional picture beside the RT picture, and if you can give me a quick answer so I can ask Mr. Connors a question.

Mr. BRILL. We could put up a dart board and put six answers on that dart board and throw a dart at one of them any day of the week and get a different answer. We have gotten six different answers.

Ms. JACKSON LEE. What do you think?

Mr. BRILL. I know, actually. An inspector came down to Orlando in the fall of 2006, just a routine inspection in Orlando, and he saw the Registered Traveler line, so people weren't showing their driver's license, and said to the federal security director what is that? He said that is the Registered Traveler line. And the inspector said what is that? And they explained to him what Registered Traveler was.

He quickly wrote a memo, which the federal security director I think sent to me, saying you have got to show a picture ID. I sent it to Mr. Hawley, or I called Mr. Hawley and said this is obviously ridiculous, this guy obviously doesn't know about registered traveler. Mr. Hawley said it is, I will check into it.

The next I knew, this is a pattern, the next I knew, what was ridiculous was suddenly unridiculous because the staff came up with six or seven reasons why.

Ms. JACKSON LEE. They had no incredible reason as you can define it.

Mr. BRILL.? They just couldn't do what the press could never do, which is admit a mistake. Screwed up.

Ms. JACKSON LEE. You do have that background. Let me just quickly ask, you recognize our job here is securing America and assuring its security. You would welcome the opportunity to refine the vetting system.

Mr. BRILL. The answer is yes, this is a voluntary program, and our members would welcome it. We would welcome it, but we have been told that before.

Ms. JACKSON LEE. We are here to start a new day and turn on the light.

Mr. Connors, very quickly, are you here supporting the Registered Traveler on behalf of business travelers?

Mr. CONNORS. Yes, absolutely.

Ms. JACKSON LEE. Would your travelers welcome a more extended vetting beyond just checking their name against a watch list?

Mr. CONNORS. I think they are under the impression that that already exists. I went through the pilot program myself here in Washington, D.C.

Ms. JACKSON LEE. It may not exist. So the question is would they be willing in your belief to take a more extensive vetting of their background?

Mr. CONNORS. Yes, I do think so because I think they believe that is happening now, and they are signing up for it in droves.

Ms. JACKSON LEE. I thank you. Let me yield now to the ranking member for 5 minutes.

Mr. LUNGREN. Thank you very much. Mr. Brill, what is the background check that goes on right now with people who sign up?

Mr. BRILL. I am delighted to say I don't know the details of it, nor should I. It is a security process that TSA is responsible for. My understanding, because I have heard it articulated in the past, is that it is much more than one watch list, as Congressman Lofgren pointed out, and it is also a wants and warrants list.

I know it is a check of citizenship because the people who sign up and who don't get it invariably is because they said they were U.S. citizens, and TSA is checking that and they find out that they are not U.S. citizens. I think Mr. Hawley was misinformed about the nature of the check.

Mr. LUNGREN. Well, the question goes to this whole issue about commercial vendors having information on people that they could go and distinguish between. One happens to be John Anderson, the former presidential candidate and gets stopped at every airport, and we had a hearing on that. The only way to exclude him is to query some systems that are more than what the government—

Mr. BRILL. Not exactly. If there are four John Andersons, what TSA wants to know or what any keeper of a watch list wants to know is which John Anderson lives in Brooklyn and which one is from whatever district he was from in Illinois, and which one is from California. It is the one who has a certain date of birth and address tied to a name that is meant to be on their watch list.

The way you find that out is through Registered Traveler. People have to show up to enroll, they have to bring their documents like their driver's license and their passport, which gets scanned through a machine looking for forgeries. We authenticate those doc-

uments before we say that you are John Anderson who lives at this address.

So we have offered to TSA, we have offered repeatedly that we will give, give a Registered Traveler card to anyone who has the problem that Senator Stevens' wife has, or that Ted Kennedy has, which is the misfortune of having a wrong name, and they are always on the list. We will give cards to them because our process separates out, if you will, the good John Andersons from the bad John Andersons.

Mr. LUNGREN. Have you sat down with TSA about this?

Mr. BRILL. Repeatedly. They don't want to get that help from a private sector program. We have done it repeatedly. We have said to TSA we got a call from an employee at DHS saying we would like to get a discount Registered Traveler card. We have said the government employees can have a discount but you can have a deeper discount, like almost for free, if TSA will simply recognize the screening you have already gone through.

We have asked TSA will you recognize the screening that DHS employees at headquarters go through? They have said no.

You laugh.

Mr. LUNGREN. I am not sure what to say to that.

Let me ask you this about the machinery that you have with GE. In the exhibit that you had over in the other building it purports to identify metal in shoes, purports to identify explosive—any sense of explosives either of the shoes or of the fingers, is that correct?

Mr. BRILL. If you have a trace of residue on the finger, and supposedly that is very sensitive. Supposedly it is. It certainly is more sensitive, just logic would say, than not doing it.

Mr. LUNGREN. And are these the two things that you have been told TSA, if it works, would accept for giving you some benefits in streamlining the security review?

Mr. BRILL. I don't want to mischaracterize any of it. TSA or GE has not promised us anything in return for anything, although TSA did announce to the press in December of 2006 that the shoe scanner had been tested and was ready to be used to vet shoes and then suddenly they changed their minds. But that is their right. They should change their minds. They shouldn't worry about being embarrassed if it is a security issue to change their mind. We just think this could be done on a faster track.

We are not—I mean I have a lot of respect for, people too, so I know what they go through every morning in that office when they get intelligence threats, I know there are people trying to do us harm through aviation, I just don't see the can-do attitude, the welcoming attitude that I saw way back, when, when I was writing about them.

Mr. LUNGREN. Thank you. Appreciate it very much. I am sorry I have to leave. We have a FISA briefing from another committee. I appreciate this presentation, and I hope that this helps us try and bridge the gap that seems to exist between TSA and the private sector that seems very evident by what is being said here at this hearing.

Mr. BRILL. There shouldn't be a gap.

Mr. LUNGREN. I agree with you. I mean I agree with—I would like to see us somehow bridge that gap. I think you will find most

members on this committee, if not all members of this committee and subcommittee, want to see that as well. Thank you very much.

Ms. NORTON. [presiding.] Thank you, Mr. Lungren. I yield myself 5 minutes. The reason I have begun to lose patience with this process is the absence of detail as to what needs to be done to either move it faster or to correct whatever problems have been found. I have lost patience because I sit on the Aviation Subcommittee, and if you sit on that subcommittee you will have to believe that the future lies in technology rather than the systems that TSA is relying on. Multiple layers, as he spoke of in his testimony.

I mean this is not Israel, a small country where you might be able to have sufficient people to do these multiple layers and be convinced that human error would not take place, and save us, please—don't talk to this committee about the watch list. Save us from the watch list, if that is the pen and paper, that list of names is what we are talking about.

I begin my question this way because very frankly the errors that we find every time that we test TSA's present technology terrifies the public. That is to say human beings are human beings, they always will be, and the devices are repeatedly found. Meanwhile, private industry develops what appears to be moving toward a fairly fool-proof technology, and we can't get any answers about what is delaying it.

Far from interesting, and I don't even have to get on the planes, every member of this committee is very interested in speeding this lineup. I am on this committee, I am on the Aviation Subcommittee, and I am terrified at what TSA is now doing in slowing up, getting us to a process that is above anything now apparently even contemplating.

So my question doesn't go to how do we move to the next level of doing some testing, I want to know from you, Mr. Conaway, and you, Mr. Brill, whether or not you think that we could in reasonable time get to the point where we use universal RT rather than RT for those who pay a hundred dollars in a business class of passengers who are leading the way.

I have lost confidence in what we are doing now and what the head of TSA seems to be depending upon to move on. I would rather accept errors from technology than the errors I see before me as a member of the Aviation Subcommittee.

So I am going for a faster track, not to slow the lines down. I am asking for a faster track for security reasons because I do not believe we can continue to tell the public that you are secure when you get on airlines, given the methodology we are now using.

Mr. BRILL. I think you can move toward what I would call universal RT, it would be RT in which you would let people who are law enforcement, members of law enforcement and other people who have already been screened, who somewhere some responsible end of the government has said these people are security safe, such as the staff on this committee, for example.

Ms. NORTON. You mean a background check?

Mr. BRILL. Why should a Secret Service agent have to pay us and have us pay TSA \$28 for him to get a background check to join Registered Traveler. That is just crazy. So I think you can have near universal RT if you involved people who are background

screened. We already offer the card for free to active duty members of the military.

Ms. NORTON. So if 70 percent of the public said I want to be background screened.

Mr. BRILL. If 70 percent of the public had EZ Pass to go over the Triborough Bridge, everybody would go faster because you have that many more EZ Pass lanes. What has to happen though is we are not asking for any security benefits because of the screening, we are just saying not add a security burden of two forms of identification. That is just insane.

Ms. NORTON. Or take off their shoes.

Mr. BRILL. We are saying if this equipment works, give it a fair shot, and if it works, it is your decision. If it works, allow people not to take their shoes off. But at least in the interim while you are testing the equipment, and for God's sake, test it on some kind of transparent schedule, stop imposing a double burden on Registered Traveler members because, people laugh at us. They say what is the purpose of my card if you are making me show my fishing license or driver's license. No one has an explanation.

Ms. NORTON. Mr. Conaway.

Mr. CONAWAY. Let me offer a slightly different take on this and separate out a background check from the security check that goes on at the checkpoint itself because there is a threat with a clean-skinned terrorist that has never—would pass a background investigation but still may do something bad.

If RT were to move forward the way industry had envisioned it, what it would open up is a means of bringing private capital into advancing the state of the art of sensing technology that could be used at the checkpoint. If we make that work for a Registered Traveler lane, then why couldn't that then be the impetus to take that same technology and now implement it in all the other lanes at the airport.

Ms. NORTON. The Federal Government will never pay for the kind of technology you are developing, sir. Never pay for it. Therefore they are paying for low tech. We will never be able to get them to pay for the kinds of things you are doing and therefore bringing private capital into it would be—

Mr. CONAWAY. The biggest problem is the largest cost there is the research and development. Once it is available for production—

Ms. NORTON. I am sorry; the President proved that is not the case. I just want to say, Madam Chair, because I want Ms. Lofgren to have a chance before you go to vote, that there is one analogy here. This same TSA refused to open, the general aviation, Reagan National, despite the Transportation Committee giving them—including a bill. Not until the chairman of the committee said that unless they issued regulations so we know if it is safe or not, he would hold them in contempt. That was 4 years after 9/11 did they open it. These folks we have heard here today are not going to let these folks move forward unless this committee makes it happen.

Thank you very much, Madam Chair.

Ms. JACKSON LEE. [presiding.] Yield to Mr. Broun for 5 minutes.

Mr. BROUN. Thank you, Madam Chair. I just have a quick question or two, Mr. Conaway, Mr. Brill, I think either one of you may

be able to answer this. Is it your gut feeling that TSA is dragging their feet because they absolutely don't want to institute an RT type program?

Mr. BRILL. I will take my government contractor friend off the hook here. I think there are two reasons; one is, and I think Kip Hawley is a terrific public servant and a sincere person. I think he has not yet grasped the fact that this is a security program, not a convenience program.

Risk management is not about providing convenience, it is about providing security. This is a risk management program. When Secretary Chertoff talks about risk management, this is the embodiment of a risk management program. I don't think he appreciates that, and his staff has done everything to misinform him about what this program is all about, even to the point where you heard him today say he hadn't heard about the 12-year-old thing, where a 12-year-old has to show two forms of ID on our line and nothing on anybody else's line.

He has gotten e-mails about that, everybody knows about that. It has been the subject of a lot of discussion, a lot of complaints from our customers. So I think it is a combination of he is misinformed. He has not made it a priority because he sincerely believes it is a convenience program, not a security program.

I think if you can take 30 to 50 percent of the people moving through an airport and test them for traces of explosives and test their shoes and know their biometrics and know their identities, that is a security program.

Mr. BROWN. Can you assure the American public that with the current level of technology, that these people are going to be secure with what you have right now?

Mr. BRILL. Risk management is not about the elimination of risk. There is no way that anyone conducting any kind of security program in the United States can assure anyone. We can't be sure that a Secret Service man isn't going to have a problem in the White House.

I can assure you that we are completely in agreement with the idea that TSA ought to make the decisions about the security. We are not asking them to make a certain kind of decision. I don't know anything about that technology. I would be the last person on Earth you would want to have say use that and don't make people take off their shoes.

There are a lot of very good experts at GE and elsewhere and in labs, including TSA's own chief technology officer in December of 2006, who said it was very good security. We are just asking for crisp, transparent, fair decisions by people who actually want the program to work, don't see it as some burden of some pesky business people who just want to get convenience for 1 or 2 percent of the population.

Mr. BROWN. T1 SO YOUR LEVEL OF SECURITY IS AS HIGH OR BETTER?

Mr. BRILL. We think it is better. We are not asking for—the benefit we are asking for today is don't make us show two forms of identification, make us show one the way everybody else does. That is today's benefit. We are asking for a test of the equipment. That is not an unreasonable benefit. We just want to show one form of

identification that happens to be biometrically secure as opposed to a fishing license or the Orlando Public Library library card or the library card of Kazakhstan. There are no standards for those photo IDs. That is all we are asking for today.

Mr. BROWN. Thank you. Madam Chairwoman, I yield back.

Ms. JACKSON LEE. We do have a vote on the floor. We would like to finish this hearing.

Ms. Lofgren.

Ms. LOFGREN. I will be very quick. Thank you, Madam Chairwoman, and thank you again for holding this hearing that I think has been very useful.

There is something here that doesn't make sense to me and I am wondering, Mr. Brill, you have been outspoken here, and logical. Why do you think TSA is doing what it is doing? The standards are issued yesterday, I have got to suspect that is because the hearing was today.

Mr. BRILL. Of course.

Ms. LOFGREN. Why is it developed in this way?

Mr. BRILL. It goes back, I knew you were going to ask a question like that because we have had a conversation akin to that. I was thinking about 6, 8 months ago I got a call or we got a notice from the TSA, this credentialing office, we are going to have an industry day meeting, please be here at 9:00 tomorrow. Something dawned on me. These people think that I am some government contractor hanging around Washington ready to go talk to the boss of the government who pays my bills and if they called a meeting for 9:00, I just better get there at 9:00, and if they change it to 11:00, or make us wait, we will do that too.

The basic attitude is that they, the government programs, are to be paid for by taxpayers and here we are doing something, and not just Unisys and a lot of people, doing something that is creative and that is not a government program and I just think they don't like it. I don't think it has anything to do with anything really other than that. Their directives are confusing, illogical. The best one is the 12-year-old having to show two pictures.

Ms. LOFGREN. It doesn't add up. I guess the question I further have is how are we going to—we have had this hearing today, it is important, but in the history of the Department of Homeland Security you have a hearing and then nothing happens. And so we all know it because we have been on the committee now for a long time. And the lack of performance in the Department generally is stunning.

I would invite, I know we have a vote and I don't want to go on, but I would invite the comments or thoughts of all three witnesses on suggestions on what we might do to set this thing right. I think there is an interest on a bipartisan basis to do that.

When I walk by every Monday morning at the San Jose airport I would like to think we accomplished something in the committee instead of not.

I thank the gentlelady for yielding and for my opportunity to participate in this subcommittee hearing. I will yield back because we do have to get to the floor to vote.

Ms. JACKSON LEE. Ms. Lofgren, let me thank the members of this committee.

All of you have provided very instructive, and all of the members have had very instructive questioning. This is a good hearing.

I will accept the challenge from Congressman Lofgren before I close the hearing, pose just a question and then say to you that we are not going to go from the bottom up. Frankly, this is a problem that has to be solved for the security of Americans, and I think we do a disservice to 21st century security if we ignore technology. And frankly there seems to be a disconnect.

This has been an instructive and enlightening hearing, primarily because we have found part of the crux of the problem and it seems to be in contrast to the Science and Technology Assistant Secretary who is traveling all over the country looking for innovative technology to secure America.

So let me just very quickly ask, Mr. Connors has gotten on record that he is supportive of a process that improves technology and moves business travelers along. Let me make sure Mr. Conaway is not saying something differently regarding technology, and you would have no problem to GE meeting the standards of TSA and using an RT program that might in fact take up to 70 percent of America's population, traveling public. Would that be something you would oppose?

Mr. CONAWAY. No, ma'am.

Ms. JACKSON LEE. Mr. Brill, we have spoken about sophisticated business travelers and you have spoken about the Secret Service and FBI and others, but there is the 90-year old—or maybe a 50-year old; let me go to the 90-year old, with an artificial hip, leg or otherwise, but still going.

These kinds of inconsistencies that we find in our traveling public that are facing—that they face with regards to security. I don't think I have preempted the fact that we are stopping people with breast milk and some other things come August 4th.

Can you work with the idea that we begin to look top down and take this to the policymakers of the agency so that we can frame the best way to make RT work? Would the private sector work with us on that?

Mr. BRILL. Yes, ma'am. That in fact was the idea we had when we offered TSA tell us who you have adjudicated off of the threat list, off of the watch list, which is something that caseworkers in all of your offices have to deal with every day, and if they want to, they can volunteer. We will give them Registered Traveler cards for free, which is the only way that adjudication works.

By the same token, if someone has some metal in a leg or something else, if TSA will adjudicate those people and instruct them to give—instruct them that they qualify for a card, we would do that. We see the public service in sort of a selfish way, which is we want TSA and the government to support this program and support voluntary credentialing so we would, as with people on the threat list, we would give, give the card to those people. You shouldn't have to pay us a hundred dollars because you have the bad luck to have a bad name and you are on a threat list. As long as TSA will tell us that. They just turn us down.

Ms. JACKSON LEE. Let me just say that I think we need to end on the note that this committee will not leave this unattended to. We want to achieve the highest level of security for the RT pro-

gram but, frankly, I think as some of my colleagues have indicated, I am interested in a vastly expanded program only because I want the resources of the Transportation Security Administration focused on those who are going to attempt, as the National Intelligence Estimate has said, to do this country harm and to create havoc and to create a terrific, horrific terrorist act.

So let me conclude by saying that this will be, I guess, the first of the beginning of how we address the question on the RT program. Let me thank the witnesses for their valuable testimony and the members for their questions. Members of the subcommittee may have additional questions for the witnesses. We will ask you to respond expeditiously in writing so that those questions can be answered.

Hearing no further business, the subcommittee now stands adjourned.

[Whereupon, at 4:45 p.m., the subcommittee was adjourned.]

