S. HRG. 109–461

THE TRANSPORTATION SECURITY ADMINISTRATION'S AVIATION PASSENGER PRESCREENING PROGRAMS: SECURE FLIGHT AND REGISTERED TRAVELER

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

FEBRUARY 9, 2006

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

U.S. GOVERNMENT PRINTING OFFICE

27–562 PDF WASHINGTON : 2006

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

TED STEVENS, Alaska, *Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
KENNETH R. NAHIGIAN, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

CONTENTS

WITNESSES

APPENDIX

THE TRANSPORTATION SECURITY ADMINISTRATION'S AVIATION PASSENGER PRESCREENING PROGRAMS: SECURE FLIGHT AND REGISTERED TRAVELER

THURSDAY, FEBRUARY 9, 2006

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m. in room SD–562, Dirksen Senate Office Building, Hon. Ted Stevens, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Senator INOUYE. The Chairman of this Committee is presently presiding at the U.S. Senate in his capacity as President pro tempore, so he sends his regrets he cannot be with you.

The TSA has spent hundreds of millions of dollars on Secure Flight, Registered Traveler, and other airline passenger prescreening programs, yet we have been told that there are few tangible improvements in security to show for this investment.

With respect to Secure Flight, Congress outlined specific privacy, security, and spending requirements for the agency to meet before moving forward with the program. Despite the TSA's assurances that it would be operational within the year, Secure Flight has yet to be implemented.

The Registered Traveler Program has experienced similar setbacks. The Nation's air carriers have begun to call into question the necessity of the program. Others have raised concerns about the impact of the program on existing airport screening systems, and have questioned whether or not the program will produce an equitable and more secure program.

To date, no one at the TSA has taken responsibility for this, and the lapses have squandered scarce public resources and delayed important security improvements. These programs make sense, in theory, and we know that related technology is available. But will the traveling public ever realize the stated benefits? So, we need a far more candid and honest assessment than we have received thus far, and I look forward to hearing from Mr. Hawley about his next course of action.

But before I call upon you, sir, Senator Lott?

STATEMENT OF HON. TRENT LOTT,
U.S. SENATOR FROM MISSISSIPPI

Senator LOTT. Thank you, Senator Inouye—"Co-Chairman," I believe is the way we describe your title on this Committee. It's a real pleasure to see the way you and Senator Stevens work together. I think it's in the best interest of the Senate, and I wish more people would follow your example.

Thank you for being here this morning. I'm looking forward to hearing the witnesses' testimony we have before us now, and hopefully even the next panel, even though I do have an Intelligence Committee hearing I must attend. And so, I thank all of you for being here, and I will review your statements that you have.

You know, I'm quite often quick to be critical, and I have certainly been critical many, many times, and with lots of justification, of the TSA. But I think, Mr. Hawley, that you're trying to get it turned around. I see some small signs of a little common sense kicking in. Not a lot. But that's the way it works in the Federal Government. Even if you get good, strong leadership at the top, it doesn't seem to always get all the way down to the people on the ground, or to the gate, in the case of the airlines. But you've taken some criticism for the new screening procedures and changes to the prohibited-items list, and I want to make it clear, I think you did the right thing. I think you still haven't done enough. I don't know how many of my little pen knives I'm going to have confiscated, but I lost another one this past weekend. So, I just buy 'em by the dozen now.

[Laughter.]

Senator LOTT. I do realize this is a serious threat to airlines, but I've gone from the black ones to the white ones, so I've got plenty of them.

But you made some little small change. I mean, you've got all my little scissors. If you could just send them in a big box, I could probably use them. But you're trying to do the right thing, and I want you to know that I appreciate it. I appreciate your attitude. And I appreciate the fact that you did something to begin to bring some modicum of common sense to the gates.

Let me make just a couple of more points, then go to your testimony.

I do want to make it clear that I'm absolutely opposed to the Administration's suggestion to increase passenger security fees again. Congress rejected it last year. We're going to reject it this year. Why waste your time, your breath, to suggest such a thing? Because the airlines have got enough problems without that being added to it. Plus, I don't think you need more money. I don't think TSA needs more money. You need to do a better job with what you have. The budget request for 2007 is 4.607 billion. So, I think you need to find ways to do a better job with less money.

And part of it is to quit fumbling around with things and make a decision, make it happen. How long do you—look, I could come over with a pencil and a napkin and design a program for the Registered Traveler Program. At least you're trying to make it work, but—I think—but now you've got milestones you've got to meet, and we may be able to get it in place by June. You get no awards for that. What's wrong with April? What's wrong with next week?

Get on with it. Because it's—it wastes time and energy and money, and I don't understand why it should be so hard to do that.

Now, I guess the argument is going to be, from you and some people, "Well, we're getting pushback because of privacy advocation concerns." Forget that. If people don't want to divulge their private information for this voluntary program, fine, they don't get in it. I don't understand what people are trying to hide. Get on with this.

And that's part of the problem, overall. I mean, you—the Secure Flight thing, we've been messing around with the CAPPS II and Secure Flight for 4 years, 200—between 200 and 300 million. Do something, even if it's wrong. And part of the problem, for instance, with regard to this—the registered flyer program is, industry officials really don't think you're dedicated to moving the program forward; you really don't want to do it, for some reason. I don't know what it is. I don't know if they know what it is. But enough money spent, let's get some action. And we want to help you every way we can, and not be an impediment and a pain in your neck. I only call you and scream at you from BWI once a year.

[Laughter.]

Senator LOTT. So—but it could increase.

But we want you to succeed, because it's very important work you do. We want secure flights, but we want some common sense applied in how people are screened and what the conditions are for flying. Let's do some of these programs, or forget them, but quit fumbling around with them.

Thank you for the opportunity to ventilate a little bit, Mr. Co-Chairman, and I'll look forward to hearing the testimony.

Senator INOUYE. Thank you very much.

Senator Lautenberg?

STATEMENT OF HON. FRANK R. LAUTENBERG, U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Yes, thanks very much, Mr. Chairman.

And I guess that's wishful thinking. But to Senator Lott, talking about the confiscation of that weapon he's carrying there, the fact of the matter is that I think this was originally a scheme by the scissor manufacturers to make sure that there was always an opportunity to replace them. But in any event, the nuisance side of things is really just a plain pain in the neck, and we've seen that, now, scissors aren't the weapon that they were intended to be. I'd trade in your knife for a pair of scissors. I think that's probably the best way. But the fact is that we've got to get on with securing our aviation system and to make it more secure for passengers.

My state lost 700 people in 9/11. Many people in New Jersey could see the flames and smoke at the World Trade Center from their homes and offices. And I was a Commissioner of the Port Authority before I came here; we had offices in the Trade Center. My home in New Jersey is right across the river from where the World Trade Center was. The absence of those two towers is obvious. The towers can be replaced, but the pain felt by the families can never be dealt with appropriately.

After 9/11, we realized that our aviation system was not as safe and secure as it needs to be. We learned that some of the hijackers were known terrorists who never should have been allowed to

board a commercial flight. And that's why this Committee created the Transportation Security Administration, and why we continue to oversee its activities.

We must be certain that the American people, neighbors and our families, can travel safely. Considering the importance of this mission, I share the words of Senator Inouye, and say that I'm disappointed by the Administration's lack of progress in securing our transportation systems. Most of TSA's resources have been directed toward aviation security. And when it comes to aviation, it would seem that TSA's top priority should be to know when a suspected terrorist, or at least someone on the list, is attempting to board an airplane. And this fact was highlighted a few months ago when a man at Newark Airport got on a plane without even holding a valid ticket. He had taken a printed fare estimate that he got at the airline ticket counter, and used it, along with his ID, to board an airplane. If he had been a terrorist, we might not have known until it was too late. This lapse by both the airline and TSA highlights the importance of prescreening passengers, weeding out the few suspected threats from the millions of travelers that move each day.

Now, I'd like to see a working passenger prescreening program that properly and efficiently matches passenger names with the suspected terrorist list. But this seems to be more of a challenge for TSA than anticipated.

And as for the Registered Traveler Program, those of us who fly frequently would very much like a way to speed the process up for the kind of frequent flyers, as we call them. I don't mean to say that those who spend the most money ought to get the best attention, but the fact is that those who travel frequently by air are easier to identify, and we ought to get on with doing that.

So, Mr. Chairman, this is a timely hearing. I look forward to hearing from our witnesses and hope that we can see some progress pretty soon.

The CHAIRMAN. [presiding] Senator Nelson, do you have an opening comment?

STATEMENT OF HON. E. BENJAMIN NELSON,
U.S. SENATOR FROM NEBRASKA

Senator BEN NELSON. Mr. Chairman, thank you very much.

Just one observation. Going through an airport recently, I found that there were two lines. There was a line for those who flew first class and those who flew non-first class. Two different lines going through the same security screening process. Since I think we all pay the same amount for the screening process, I couldn't understand the distinction between first-class lines to get through and the others. I can understand getting—riding in the—flying in the front of the plane, but I couldn't understand that. And so, I'd like Mr. Hawley to be thinking about that before we get to the questions.

Thank you very much. And I appreciate also having this opportunity for this hearing.

The CHAIRMAN. Thank you very much.

OPENING STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The CHAIRMAN. I apologize for being late. I was in the Chair of the Senate. My relief was a little tied up in traffic.

I think we should all recognize this is a first in a series of hearings on aviation security. The next hearing will be on March 9th, when we continue the evaluation of the airline passenger screening programs and examine the physical screening of airline passengers and their baggage.

The purpose of today's hearing is to examine two of TSA's commercial aviation passenger screening programs, Secure Flight and Registered Traveler. The emphasis on today's discussion I hope will be to review the policy and management issues that have prevented TSA from launching these programs, to determine the future of the programs.

I do support the Administration's efforts to secure all modes of transportation, as well as any program that yields a significant security benefit to Americans, comparative to the cost of developing and operating the program. The programs at issue today have been in development now for 4 years, and, for various reasons, have not yet come to fruition.

The Committee is going to seek answers from the witnesses here today regarding the cost of Secure Flight and the Registered Traveler Program and the necessity and viability of the programs, and the timetables related to them.

I'm going to print the rest of my statement in the record.

[The prepared statement of Senator Stevens follows:]

PREPARED STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

We welcome the witnesses who will appear before the Committee today, and thank them for their willingness to participate in this hearing.

Today represents the first in a series of hearings that the Committee will hold on aviation security. On March 9th, the Committee will continue its evaluation of TSA airline passenger screening programs, and examine the physical screening of airline passengers and their baggage. That hearing also will deal with screening technology, screener workforce issues, and TSA procurement processes.

The purpose of today's hearing, however, is to examine two of TSA's commercial aviation passenger pre-screening programs, Secure Flight and Registered Traveler. The emphasis of today's discussion will be to review policy and management issues that have prevented TSA from launching these programs, and to determine the future of the programs.

I support the Administration's efforts to secure all modes of transportation, as well as any program that yields a significant security benefit to Americans comparative to the cost of developing and operating the program. But the programs at issue today have been in development for four years and, for various reasons, have yet to come to fruition.

The Committee will seek answers from the witnesses regarding the costs associated with Secure Flight and Registered Traveler, the necessity and viability of the programs, and the timetables for their launch. The Committee also will examine the impediments that have caused delays, including privacy concerns, and even Congressionally imposed hurdles.

I look forward to a constructive dialogue with the witnesses.

The CHAIRMAN. We're pleased to recognize the first panel: Edmund "Kip" Hawley, the Assistant Secretary for Transportation Security, and Cathleen Berrick, who's the Director of Homeland Security and Justice for GAO.

We'll call on you first, Kip. Thank you for your statement.

Your statements will be printed in the record in full. We appreciate the extent to which you can really reduce them down to approximately 5 minutes.

STATEMENT OF HON. EDMUND "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION

Mr. HAWLEY. Good morning, Mr. Chairman, Co-Chairman Inouye, Members of the Committee. Thank you for the opportunity to discuss Secure Flight and the Registered Traveler Programs.

In December's hearing, we discussed the 14 layers of protection now in place for cockpits and passenger cabins, and our view of the current risk environment. These layers range from measures the government takes overseas to preempt attacks to the security measures in place on the aircraft itself. Today, I'm here to assist the Committee in considering activities toward the middle of the 14 layers, passenger prescreening.

Passenger prescreening can be broken down into three parts:

One, identify known terrorists and prevent them from getting near the aircraft. This is the role of watch-list-matching, which is now done by airlines and will be transferred to the Government under Secure Flight.

Second is to identify behaviors common to terrorists whose names we don't know, and give them additional screening. This is the role of the computer-assisted passenger prescreening, or CAPPS, process.

Third is to identify people who do not pose a threat to aviation security, so that we do not expend valuable security resources unnecessarily. This is the role of Registered Traveler.

Secure Flight is the most important of these, and also the one requiring the most management attention. I'll focus my opening remarks on Secure Flight.

The effort to improve terrorist watch-list screening, first through CAPPS II and subsequently under Secure Flight, was, and is, a complicated task. Despite sincere and dedicated efforts by TSA, there has been an undercurrent of concern from outside stakeholders really from the beginning. Over the past 4 years, many concerns have been raised and addressed, but Secure Flight continues to be a source of frustration.

Congress recognized these issues when it included special certification requirements for the Secure Flight Program in recent appropriations acts, and we appreciate GAO's efforts to provide a comprehensive review of the Secure Flight Program.

We are in the process of making changes to how TSA operates, aligned with Secretary Chertoff's risk-based strategy for the Department. I've previously shared with you our overall strategy, organization changes that support that strategy, and in December we reviewed some of the operational steps that are now in action.

As part of this continuing review, I asked TSA's Information Technology Office to conduct IT system security audits of all TSA credentialing and vetting programs. This review, which includes Secure Flight, is ongoing, but I believe it is safe to say that many of the same issues identified by GAO are also highlighted by this more detailed review.

Rather than address any identified weakness on its own, I have directed that the Secure Flight IT systems go through the comprehensive recertification process pursuant to the Federal Information Security Management Act, FISMA, requirements. This action and the others we're taking, I believe, is compatible with GAO's suggestions that we rebaseline the program and ensure that we use technology-development best practices in management, security, and operations. While the Secure Flight regulation is being developed, this is the time to ensure that Secure Flight's security, operational, and privacy foundation is solid.

We will move forward with the Secure Flight Program as expeditiously as possible, but in view of our need to establish trust with all of our stakeholders on the security and privacy of our systems and data, my priority is to ensure that we do it right, and not just do it quickly.

When I appeared before the Committee during the confirmation process, I said that I believe programs like Secure Flight should be built from a strong privacy foundation as a starting point, as opposed to building it and then adding privacy. The approach I just outlined will accomplish that. Security and privacy are necessary ingredients of each other, and not opposite ends of the spectrum. TSA will approach all of its programs with that in mind.

On Registered Traveler, I will just say that it will be market-driven and offered by the private sector. TSA's principal requirements are that, one, it pays its own way, and, two, does not diminish security. We are fully aware that terrorists may attempt to exploit Registered Traveler Program benefits, and the program is designed to thwart those efforts.

On November 3, 2005, I outlined the path forward for Registered Traveler. We are on track, having met the milestones established for January 20th. Depending on the pace of our market-driven private-industry partners, TSA expects to be ready to begin screening Registered Traveler Program applicants by mid-June.

Mr. Chairman, I look forward to working with you and the Committee.

Thank you.

[The prepared statement of Mr. Hawley follows:]

PREPARED STATEMENT OF HON. EDMUND "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION

Good morning Mr. Chairman, Co-Chairman Inouye, and Members of the Committee. I am pleased to have the opportunity to appear before you today on behalf of the Transportation Security Administration (TSA) to discuss non-physical security screening programs. As requested, my testimony will focus on the Secure Flight and Registered Traveler programs, two promising programs that can play an important role in our comprehensive, multi-layered aviation security network.

Last fall, before this Committee, I shared the key principles that are guiding the work and priorities of TSA. Secure Flight and Registered Traveler are rooted in two of these principles: using risk/value analysis to make investment and operational decisions, and making the best possible use of coordinated interagency intelligence and information.

Secure Flight will enhance our ability to identify known or suspected terrorists before they attempt to pass through the airport security checkpoint. It builds upon the work of the law enforcement and intelligence agencies who provide the information necessary to prescreen passengers, and recognizes that our strongest defense against terrorism is to detect terrorists before an attempt to attack.

Registered Traveler focuses on people at the other end of the threat spectrum. It is intended to enable people who are not considered threats to aviation security to move more quickly through the security process. The program is expected to reduce the time and resources that must be devoted to screening such individuals at the airport screening checkpoint, allowing TSA to focus more attention and resources on people we know less about and who may pose a greater threat to aviation security.

Secure Flight

Computerized screening of airline passengers predates the creation of TSA. The Computer-Assisted Passenger Prescreening System (CAPPS), a joint effort by airlines and the Federal Government, has been used to screen passengers since the mid-1990s. The CAPPS program uses an algorithm that draws upon information in passenger name records (PNRs) to determine whether a passenger and his or her property should receive a higher level of security screening prior to boarding an aircraft.

The Aviation and Transportation Security Act (ATSA) (Pub. L. 107–71), which created TSA, mandated that computerized passenger prescreening continue on an expanded basis. Since 9/11, we have added more comprehensive computerized prescreening measures and enhanced CAPPS processing rules. Today, airlines must also compare passenger names to the names on two consolidated Federal Government watch lists known as the No-Fly and Selectee lists. These watch lists are the product of an on-going interagency effort, and are maintained by the Terrorist Screening Center, a multi-agency center administered by the Federal Bureau of Investigation (FBI). TSA continues to work closely with the Terrorist Screening Center to ensure that the watch lists are accurate and comprehensive. In addition, TSA maintains a list of individuals who have a similar name to someone on the watch list, but who have already been distinguished from that person through TSA's redress process. These lists are made available to air carriers on a daily basis for use in carrying out the watch list matching function.

When an air carrier finds a passenger with a name on the Selectee list, the carrier must identify that passenger to TSA for enhanced screening at the checkpoint. When an air carrier finds a passenger has a name identical or similar to a name on the No-Fly list, the carrier must contact TSA in order to verify whether the passenger is actually the individual of interest to the government. If it is determined that the passenger is in fact the individual named on the No-Fly list, the carrier is prohibited from transporting that passenger and may contact law enforcement. As there are no children on the watch list, TSA permits airlines to deselect children under 12 without contacting TSA. TSA runs a 24-hour/7-day watch center to coordinate the resolution of issues related to watch list matches and other operational matters.

As recommended by the 9/11 Commission and mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108–458), TSA is taking steps to assume the passenger watch list matching function from the airlines through the Secure Flight program. The CAPPS screening function will remain with the airlines.

Under Secure Flight, the watch list screening process will generally occur prior to an individual's arrival at the airport, unless he or she makes a reservation or changes a flight upon arrival at the airport. Rather than transmitting watch lists to air carriers, under Secure Flight, air carriers will transmit passenger names and a limited amount of additional identifying data for flights within the United States to a central data processing unit. Passenger names will be compared to names on the consolidated watch lists, as well as a list of individuals who have already been distinguished from persons on the watch lists through the redress process.

Similar to current practice, if an individual is confirmed as a match to the Selectee list, TSA will notify the appropriate air carrier, who is then required to take steps to identify the individual as a selectee so that TSA Transportation Security Officers can apply enhanced screening to the individual and his or her property at the checkpoint. If TSC confirms a match to the No-Fly list, TSA will notify the air carrier to refuse to issue the passenger a boarding pass. The Terrorist Screening Center will assist in the match confirmation process and may notify other agencies to initiate an operational response to the match, if appropriate.

We expect that watch list screening under Secure Flight will offer significant improvements in security, efficiency and the passenger experience. It should be noted that any individual who is identified as "No-Fly" by a government agency is not allowed to board an aircraft under the system in operation today. Nevertheless, security will be enhanced by vetting passengers against the expanded watch lists produced by the TSC, instead of the more limited lists TSA currently transmits to carriers. Further, by moving the watch list screening process within the Federal Gov-

ernment, comparisons will be made using a single system, rather than the multiple matching programs now utilized by individual airlines.

Additionally, we believe the Secure Flight system will reduce the number of passengers who are misidentified as an individual on the watch list. By incorporating a limited amount of additional passenger information in the comparison process and by offering tighter integration with TSA's redress process, we expect Secure Flight to more easily and accurately distinguish passengers with similar names from those on the watch list. TSA fully appreciates the frustration of passengers facing this false positive match issue, and we are working diligently to reduce the inconvenience these passengers experience. As part of this effort, TSA's Office of Transportation Security Redress will implement a redress process that will permit passengers who are delayed or prohibited from boarding a flight to appeal and correct erroneous information. The Office will work in consultation with stakeholders and companion offices including the TSA Office of Civil Rights and the DHS Officer for Civil Rights and Civil Liberties in implementing this process.

I also want to assure the Committee that we are fully committed to protecting passenger privacy with the deployment of Secure Flight by incorporating privacy protection features into the system design. We will follow both the letter and intent of the Privacy Act, and we will continue to design, develop, and deploy Secure Flight in consultation with TSA and DHS Privacy Officers and privacy advocates.

TSA is pursuing a phased development and deployment approach to Secure Flight. Initial development and testing of the Secure Flight matching application is nearing completion. In September and November of 2004, we published a number of documents necessary to begin testing the Secure Flight matching application, including a Privacy Act System of Records Notice (SORN) and a Privacy Impact Assessment (PIA). Testing of the matching application using historical Passenger Name Records was successful. Development and testing of TSA communication links to the Terrorist Screening Center and Customs and Border Protection (CBP), through which we intend to connect to the airlines, as well as fine-tuning of the matching application, will continue through the next phase of Secure Flight's development.

In addition to application testing, TSA conducted a separate test to determine whether the use of additional data sources produced by commercial data aggregators could be used to identify potentially inaccurate or incomplete passenger data and add an additional layer of security in passenger prescreening. As a result of those tests, commercial data analysis will not be included in the operational deployment of Secure Flight.

During the next phase, we will undertake operational testing of Secure Flight by connecting with several airline partners and vetting passenger information in real time. During this phase, participating air carriers will be required to continue screening passenger names against the watch lists that are provided to them. We are currently in the process of drafting the necessary regulatory documents to implement operational testing, including the System of Records Notice (SORN) and Privacy Impact Assessment (PIA) for Secure Flight. Once this regulatory process is concluded, operational testing will begin.

Based on the operational tests, TSA will make adjustments to the systems and operations as necessary, and prepare for the phased deployment of Secure Flight. As you may be aware, the Department of Homeland Security Appropriations Act, 2006 (Pub. L. 109–90), prohibits TSA from expending funds to deploy Secure Flight until the Secretary of Homeland Security certifies, and the Government Accountability Office (GAO) reports, that all ten of the elements contained in Section 522 of the Department of Homeland Security Appropriations Act, 2005 (Pub. L. 108–334), have been met.

We appreciate GAO's efforts to provide a comprehensive review of the Secure Flight program, especially in light of the difficulties in reviewing a complex program that is still under development. TSA intends to make the required certification after completion of operational testing, and will fully cooperate with GAO as it completes its review of Secure Flight within the 90-day post-certification reporting deadline. We are confident that Secure Flight will meet all Congressional requirements for implementation.

Registered Traveler

The Aviation and Transportation Security Act (ATSA) also directed TSA to explore options for expedited travel at airports for people who do not pose, and are not suspected of posing, a security threat.

Registered Traveler Pilot programs were initiated in five airports on a staggered basis during the summer of 2004. In partnership with Northwest Airlines, United Airlines, Continental, and American Airlines, TSA established pilot programs at

Minneapolis-St. Paul (MSP), Los Angeles (LAX), Houston Intercontinental (IAH), Boston (BOS), and Ronald Reagan Washington National (DCA). Each of the five pilot programs enrolled approximately 2,000 people, who were invited to participate by the airlines from among their very frequent fliers. Participation was limited to U.S. citizens, nationals, and lawful permanent residents, and was entirely voluntary. Participants in these TSA run pilot programs were not charged a fee. The five initial pilots ended in September 2005.

In June 2005, TSA initiated a sub-pilot program at Orlando International Airport (MCO) to test the feasibility of using a public-private partnership model for the program. The sub-pilot also tests the willingness of the public to pay a fee to participate in a Registered Traveler Program. In the Orlando sub-pilot, participants pay an annual fee of $80. Approximately 13,000 passengers have enrolled in the sub-pilot, which is still in operation.

The results of the pilot programs were positive. Tests of biometric identity verification and smart card technology demonstrated that the technology performs accurately and rapidly under airport operational conditions. Furthermore, based upon the results of the Orlando sub-pilot, we concluded that the public will accept the participation of private companies in the Registered Traveler program and that a fee-based program can attract participants.

In keeping with Congressional direction and consistent with the results of the pilot and sub-pilot programs, Registered Traveler programs will be market-driven, and offered by the private sector. Individual participation in a Registered Traveler program will be entirely voluntary, with prices established by the private sector providers.

On November 3, 2005, I shared with Congress an aggressive schedule for the development and implementation of interoperable Registered Traveler programs nationwide. On December 15, TSA issued a Request for Information to assist in the identification of one or more business models for the program that will meet the requirements for nationwide interoperability, sustainability through user fees, and scalable operations. Responses were due to TSA on January 20, 2006. Based on initial responses, TSA sought additional comments and extended the response deadline to January 30.

Also on January 20, TSA provided guidance to the industry regarding the collection of biometrics and their storage on Registered Traveler smart cards, as well as information regarding the process for seeking redress of an unfavorable eligibility or revocation decision.

Biometrics will be collected and stored in accordance with already existing standards, including Federal Technical Implementation Guidance on smart cards and the American National Standards Institute/International Committee for Information Technology Standards (ANSI/INCITS) standards for biometrics. Participants will be expected to provide images of all ten fingerprints at enrollment, with necessary accommodations for physical limitations. Templates of two or more fingerprints will be stored on smart cards for identity verification at security checkpoint kiosks. Registered Traveler program requirements will be harmonized with the DHS-State Department P.A.S.S. System (People, Access, Security, Service), the credentialing effort recently announced by Secretaries Chertoff and Rice, and other government-sponsored travel facilitation programs, as they are developed.

Redress matters will be handled by TSA's Office of Transportation Security Redress until the consolidated traveler screening redress process envisioned by the Rice-Chertoff initiative is developed and implemented. As part of the redress process, applicants pursuing an appeal may be asked to provide additional information and documents for necessary processing. Applicants will receive the results of their appeal in writing. All Registered Traveler data will be handled in compliance with the Privacy Act.

Finally, we announced that TSA intends to mandate a core security assessment for each applicant to a Registered Traveler program. If providers undertake more in-depth security background checks, TSA will authorize a variety of enhanced or time-saving participant benefits at passenger screening checkpoints. Participants may receive significant efficiency benefits over what exists today, if additional security is added by a more thorough threat assessment. Registered Traveler will also include ongoing checks of participants to ensure that TSA is notified of potentially disqualifying information available after the initial threat assessment. Furthermore, if Registered Traveler providers wish to make investments in approved screening equipment, fund additional screeners, and/or obtain space for separate Registered Traveler screening, then TSA is prepared to authorize the use of dedicated screening lanes or alternative screening locations for participants.

We are fully aware and expect that terrorists may seek to exploit Registered Traveler program benefits, and we are working to design a program to thwart those ef-

forts. Therefore, program benefits can be expected to change from time to time in order to make it difficult for terrorists to anticipate our security activities. In addition, TSA will not exempt Registered Traveler participants entirely from random selection for secondary screening.

By late April, TSA expects to select an entity to certify service providers and manage compliance, and will begin issuing necessary amendments to Airport Security Plans to establish requirements for identity verification providers. The period for parties to submit plans for achieving interoperability of Registered Traveler programs will also close at that time. TSA plans to be ready to begin screening Registered Traveler program applicants in mid-June, provided that our private industry partners have successfully enrolled applicants by that time.

Conclusion

TSA's mission is to protect the Nation's transportation systems while facilitating the movement of people and commerce. Both Secure Flight and Registered Traveler can enhance our aviation security network, and we look forward to working with the Committee to implement these promising programs.

Thank you again for the opportunity to testify today. I will be pleased to respond to questions.

The CHAIRMAN. Thank you very much.

Our next witness is Ms. Berrick.

STATEMENT OF CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. BERRICK. Thank you, Mr. Chairman, Co-Chairman Inouye, and Members of the Committee, for inviting me to discuss the development of Secure Flight, a program designed to identify domestic passengers who should be denied boarding or who should undergo additional security scrutiny prior to boarding a flight.

My testimony today focuses on the development and oversight of Secure Flight, TSA's coordination with key stakeholders that are critical to the program's success, and TSA's efforts to protect passenger rights and privacy.

Overall, our work has found that TSA faces significant challenges in implementing Secure Flight, that the system is at risk of not meeting program goals. We've found that TSA has not conducted critical activities consistent with best practices for large-scale IT systems. TSA has also not followed their own established systems development process for Secure Flight. For example, officials declared the design phase of Secure Flight complete before fully defining system requirements. As a result, it's not clear what Secure Flight capabilities will be delivered when, and at what cost, and it has been difficult to measure the extent of progress on this program.

We also found that TSA has collaborated with key stakeholders whose participation is essential to support Secure Flight, and we are encouraged by these efforts. However, these stakeholders have stated that they need more definitive information from TSA about Secure Flight requirements in order to be able to support the program.

TSA has also begun coordinating with other DHS people-screening programs in order to achieve efficiencies and commonality; however, it remains unknown what changes, if any, will be made to Secure Flight or the prescreening process as a result of these efforts.

We also found that TSA must still make key policy decisions that will significantly influence program effectiveness, including what passenger data TSA will require air carriers to provide.

Finally, Secure Flight's requirements documentation does not fully explain how passenger privacy protections will be met, and TSA has not yet issued privacy notices that describe how it will protect passenger data for an operational system. As a result, it's not possible for us to fully assess how TSA is addressing privacy concerns.

Since we last reported on Secure Flight, in March of 2005, TSA has made some progress in all of these areas, including conducting further system testing and working to establish connectivity needed to make the system operate. As Assistant Secretary Hawley just mentioned, TSA has also recently taken additional steps to instill more discipline into the development of Secure Flight, including hiring a program manager with information-systems credentials and rebaselining the program to more fully defined requirements and establish milestones and cost estimates. We believe that these activities are critical, and must be completed before Secure Flight is positioned, so that informed investment decisions can be made about this program.

Mr. Chairman, this concludes my opening statement. I would be happy to respond to any questions at the appropriate time.

[The prepared statement of Ms. Berrick follows:]

PREPARED STATEMENT OF CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. Chairman and Members of the Committee:

Thank you for inviting me to participate in today's hearing on the Transportation Security Administration's (TSA) Secure Flight program. The purpose of Secure Flight is to enable our government to protect the public and strengthen aviation security by identifying and scrutinizing individuals suspected of having ties to terrorism, or who may otherwise pose a threat to aviation, in order to prevent them from boarding commercial aircraft in the United States, if warranted, or by subjecting them to additional security scrutiny prior to boarding an aircraft. The program also aims to reduce the number of individuals unnecessarily selected for secondary screening while protecting passengers' privacy and civil liberties. My testimony today presents information on the progress TSA has made and the challenges it faces in (1) developing, managing, and overseeing the Secure Flight program; (2) coordinating with Federal and private sector stakeholders who will play critical roles in Secure Flight operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing program impacts on passenger privacy and protecting passenger rights.

My testimony is based on our past reviews of the Secure Flight program, and on preliminary results from our ongoing review of 10 issues related to the development and implementation of Secure Flight, as mandated by Public Law 109–90, and as requested by eight congressional committees.[1] (See app. 1 for a description of the 10 issues.) My testimony today updates information presented in our March 2005 report on the status of Secure Flight's development and implementation,[2] including 9 of the 10 areas of congressional interest.[3] In March 2005, we reported that TSA had made progress in developing and testing Secure Flight, but had not completed key system testing, had not finalized system requirements or determined how certain aspects of the program would operate (such as the basis on which passengers would be selected for preflight scrutiny), and had not clearly defined the privacy impacts of the program. At the time, we recommended that TSA take several actions to manage the risks associated with developing and implementing Secure Flight, including finalizing system requirements and test plans, privacy and redress requirements, and program cost estimates.

Today, I present information that suggests that, 3 years after TSA began developing a program to provide passenger prescreening, significant challenges remain in developing and implementing the Secure Flight program. The results I am pre-

senting are based on our review of available documentation on Secure Flight's systems development and oversight, policies governing program operations, and our past reports on the program, and interviews with Department of Homeland Security (DHS) officials, TSA program officials and their contractors, and other Federal officials who are key stakeholders in the Secure Flight program. We reviewed TSA's System Development Life Cycle Guidance for developing information technology systems, and other Federal reports describing best practices in developing and acquiring these systems. We also reviewed draft TSA documents containing information on the development and testing of Secure Flight, including concept of operations, requirements, test plans, and test results. My testimony is based on TSA documents received, but does not necessarily reflect all documentation that was only recently made available. In addition to the TSA documents we have reviewed, we also reviewed reports from the U.S. Department of Justice Office of the Inspector General (DOJ–OIG), which reviewed the Secure Flight program, and reports from two oversight groups that provided advisory recommendations for Secure Flight: DHS's Privacy and Data Integrity Advisory Committee and TSA's Aviation Security Advisory Committee Secure Flight Working Group. We interviewed senior-level TSA officials, including representatives from the Office of Transportation Threat Analysis and Credentialing, which is responsible for Secure Flight, and the Office of Transportation Security Redress (OTSR), to obtain information on Secure Flight's planning, development, testing, and policy decisions. We also interviewed representatives from the U.S. Customs and Border Protection (CBP) and Terrorist Screening Center (TSC)[4] to obtain information about stakeholder coordination. We also interviewed officials from an air carrier and representatives from aviation trade organizations regarding issues related to Secure Flight's development and implementation. In addition, we attended conferences on name-matching technologies sponsored by MITRE (a federally funded research and development corporation) and the Office of the Director of National Intelligence. Our work was conducted from April 2005 to February 2006 in accordance with generally accepted government auditing standards.

Summary

In developing and managing the Secure Flight program, TSA has not conducted critical activities in accordance with best practices for large-scale information technology programs. Specifically, TSA has not followed a disciplined life cycle approach in developing Secure Flight, in which all phases of the project are defined by a series of orderly phases and the development of related documentation. Program officials stated that they have instead used a rapid development method that was intended to enable them to develop the program more quickly. However, as a result of this approach, the development process has been ad hoc, with project activities conducted out of sequence. For example, program officials declared the design phase complete before requirements for designing Secure Flight had been detailed. Our evaluations of major Federal information technology programs, and research by others, has shown that following a disciplined life cycle management process decreases the risks associated with acquiring systems. As part of the life cycle process, TSA must define and document Secure Flight's requirements—including how Secure Flight is to function and perform, the data needed for the system to function, how various systems interconnect, and how system security is achieved. We found that Secure Flight's requirements documentation contained contradictory and missing information. TSA officials have acknowledged that they have not followed a disciplined life cycle approach in developing Secure Flight, and stated that they are currently rebaselining the program to follow their standard Systems Development Life cycle process, including defining system requirements. We also found that while TSA has taken steps to implement an information security management program for protecting Secure Flight information and assets, its efforts are incomplete, based on Federal standards and industry best practices. Without a completed system security program, Secure Flight may not be adequately protected against unauthorized access and use or disruption, once the program becomes operational. Finally, TSA is proceeding with Secure Flight development without an effective program management plan that contains current program schedules and cost estimates. TSA officials stated they have not maintained an updated schedule in part because the agency has not yet promulgated a necessary regulation requiring commercial air carriers to submit certain passenger data needed to operate Secure Flight, and air carrier responses to this regulation can impact when Secure Flight will be operational and at what cost. While we recognize that program unknowns introduce uncertainty into the program-planning process, uncertainty is a practical reality in planning all programs and is not a reason for not developing plans, including cost and schedule estimates that reflect known and unknown aspects of the program. Further, several

oversight reviews of the program have been conducted and raise questions about program management, including the lack of fully defined requirements. TSA has recently taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, including hiring a program manager with information systems program management credentials, and more completely defining system requirements and a program management plan, including the development of schedules and cost estimates.

TSA has taken steps to collaborate with Secure Flight stakeholders whose participation is essential to ensuring that passenger and terrorist watch list data are collected and transmitted for Secure Flight operations, but additional information and testing are needed to enable stakeholders to provide the necessary support for the program. TSA has, for example, drafted policy and technical guidance to help inform air carriers of their Secure Flight responsibilities, and has begun receiving feedback from the air carriers on this information. TSA is also in the early stages of coordinating with U.S. Customs and Border Protection and the Federal Terrorist Screening Center on broader issues of integration and interoperability related to other people-screening programs used by the government to combat terrorism. In addition, TSA has conducted preliminary network connectivity testing between TSA and Federal stakeholders to determine, for example, how information will be transmitted from CBP to TSA and back. However, these tests used only dummy data, and were conducted in a controlled environment, rather than in a real-world operational environment. According to CBP, without real data, it is not possible to conduct stress testing to determine if the system can handle the volume of data traffic that will be required by Secure Flight. TSA acknowledged it has not determined what the real data volume requirements will be, and cannot do so until the regulation for air carriers has been issued and their data management role has been finalized. All key program stakeholders also stated that additional information is needed before they can finalize their plans to support Secure Flight operations. A TSC official stated, for example, that until TSA provides estimates of the volume of potential name matches that TSC will be required to screen, TSC cannot make decisions about required resources. Also, ongoing coordination of prescreening and name-matching initiatives with CBP and TSC can impact how Secure Flight is implemented.

In addition to collaborating with stakeholders, TSA has, over the past 11 months, made some progress in evaluating factors that could influence system effectiveness. However, several activities are under way, or are to be decided, that will also affect Secure Flight's effectiveness, including operational testing to provide information about Secure Flight's ability to function. TSA has been testing name-matching technologies to determine what type of passenger data will be needed to match against terrorist watch list data. These tests have been conducted thus far in a controlled, rather than real-world environment, using historical data, but additional testing is needed to learn more about how these technologies will perform in an operational environment. In addition, due to program delays, TSA has not yet conducted comprehensive end-to-end testing to verify that the entire system functions as intended, although it had planned to do so last summer. TSA also has not yet conducted stress testing to determine how the system will handle peak data volumes. In addition, TSA has not made key policy decisions for determining the passenger information that air carriers will be required to collect, the name-matching technologies that will be used to vet passenger names against terrorist watch list data; and thresholds that will be set to determine the relative volume of passengers who are to be identified as potential matches against the database. TSA plans to finalize decisions on these factors as system development progresses. However, until these decisions are made, data requirements will remain unsettled and key stakeholders—in particular, air carriers—will not have the information they need to assess and plan for needed changes to their systems to interface with Secure Flight. On the issue of data quality and accuracy, while the completeness and accuracy of data contained in the government's terrorist screening database can never be certain—given the varying quality of intelligence information gathered, and changes in this information over time—TSC has established some processes to help ensure the quality of these data. However, in a review of the TSC's role in Secure Flight, the Department of Justice Office of Inspector General found that TSC could not ensure that the information contained in its databases was complete or accurate. According to a TSC official, TSA and TSC plan to enter into a letter of agreement that will describe the data elements from the terrorist-screening database, among other things, to be used for Secure Flight. To address accuracy, TSA and TSC plan to work together to identify false positives—passengers inappropriately matched against data contained in the terrorist-screening database—by using intelligence analysts to monitor the accuracy of data matches. An additional factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system's inability to iden-

tify passengers who assume the identity of another individual by committing identity theft, or who use false identifying information. Secure Flight is neither intended to nor designed to address these vulnerabilities.

Because Secure Flight's system development documentation does not fully address how passenger privacy protections are to be met, it is not possible to assess potential system impacts on individual privacy protections. The Privacy Act and the Fair Information Practices—a set of internationally recognized privacy principles that underlie the Privacy Act—limit the collection, use, and disclosure of personal information by Federal agencies. TSA officials have stated that they are committed to meeting the requirements of the Privacy Act and the Fair Information Practices. However, it is not yet evident how this will be accomplished because TSA has not decided what passenger data elements it plans to collect, or how such data will be provided by stakeholders. Further, TSA is in the process of developing but has not issued the systems of records notice, which is required by the Privacy Act, or the privacy impact assessment, which is required by the E-Government Act, that would describe how TSA will protect passenger data once Secure Flight becomes operational. Moreover, privacy requirements were not incorporated into the Secure Flight system development process in a manner that would explain whether personal information will be collected and maintained in the system in a manner that complies with privacy and security requirements. In our review of Secure Flight's system requirements, we found that privacy concerns were broadly defined in functional requirements documentation, which states that the Privacy Act must be considered in developing the system. However, these broad functional requirements have not been translated into specific system requirements. TSA officials stated that they are completing work on integrating privacy and requirements into the Secure Flight system as the program is being developed, and that new privacy notices will be issued in conjunction with a forthcoming regulation prior to proceeding with the system's initial operating capability. Until TSA finalizes these requirements and notices, however, privacy protections and impacts cannot be assessed. TSA is also determining how it will meet a congressional mandate that the Secure Flight program include a process whereby aviation passengers determined to pose a threat to aviation security may appeal that determination and correct erroneous information contained within the prescreening system. According to TSA officials, no final decisions have been made regarding how TSA will address the redress requirements, but information on the process will be contained within the privacy notices released in conjunction with the forthcoming regulation.

Background

TSA is responsible for securing all modes of transportation while facilitating commerce and the freedom of movement for the traveling public. Passenger prescreening is one program among many that TSA uses to secure the domestic aviation sector. The process of prescreening passengers—that is, determining whether airline passengers might pose a security risk before they reach the passenger-screening checkpoint—is used to focus security efforts on those passengers that represent the greatest potential threat. Currently, U.S. air carriers conduct passenger prescreening by comparing passenger names against government-supplied terrorist watch lists and applying the Computer-Assisted Passenger Prescreening System rules, known as CAPPS rules.[5]

Development of Legacy Passenger Prescreening Systems

Following the events of September 11, and in accordance with the requirement set forth in the Aviation and Transportation Security Act that a computer-assisted passenger prescreening system be used to evaluate all passengers before they board an aircraft,[6] TSA established the Office of National Risk Assessment to develop and maintain a capability to prescreen passengers in an effort to protect U.S. transportation systems and the public against potential terrorists. In March 2003, this office began developing the second-generation computer-assisted passenger prescreening system, known as CAPPS II, to provide improvements over the current prescreening process, and to screen all passengers flying into, out of, and within the United States.

Based in part on concerns about privacy and other issues expressed by us and others, DHS canceled the development of CAPPS II in August 2004 and shortly thereafter announced that it planned to develop a new passenger prescreening program called Secure Flight. In contrast to CAPPS II, Secure Flight, among other changes, will only prescreen passengers flying domestically within the United States, rather than passengers flying into and out of the United States. Also, the CAPPS rules will not be implemented as part of Secure Flight, but rather the rules will continue to be applied by commercial air carriers. Secure Flight will operate on

the Transportation Vetting Platform (TVP)[7]—the underlying infrastructure (hardware and software) to support the Secure Flight application, including security, commonality, and data management; and, is to perform the functions associated with receiving, vetting, and returning requests related to the determination of whether passengers are on government watch lists. This application is also to be configurable—meaning that it can be quickly adjusted to reflect changes to workflow parameters. Aspects of Secure Flight are currently undergoing development and testing, and policy decisions regarding the operations of the program have not been finalized.[8]

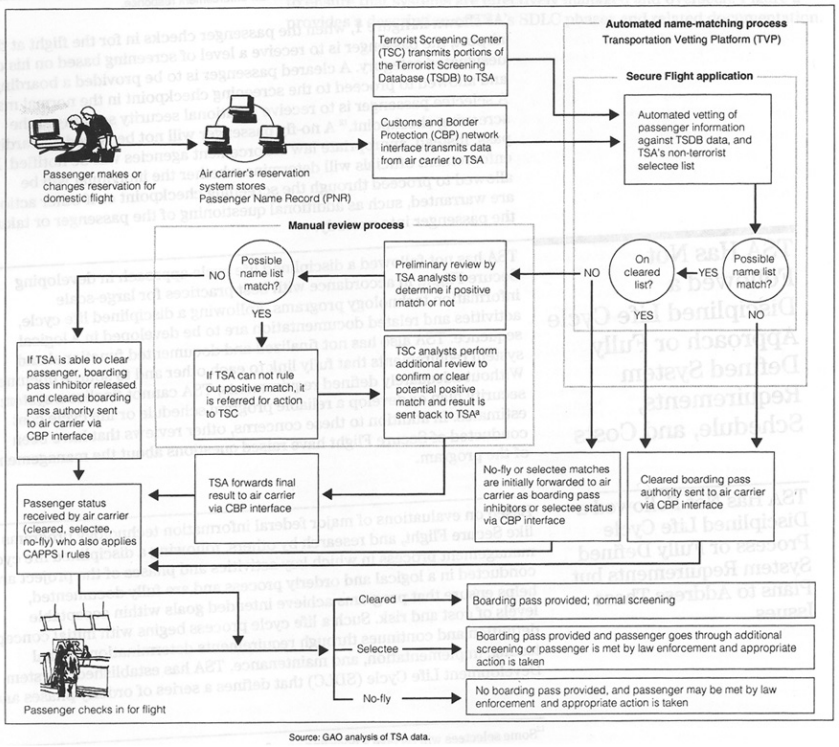
Overview of Secure Flight Operations

As currently envisioned, under Secure Flight, when a passenger makes flight arrangements, the organization accepting the reservation, such as the air carrier's reservation office or a travel agent, will enter passenger name record (PNR) information obtained from the passenger, which will then be stored in the air carrier's reservation system.[9] While the government will be asking for only portions of the PNR, the PNR data can include the passenger's name, phone number, number of bags, seat number, and form of payment, among other information. Approximately 72 hours prior to the flight, portions of the passenger data contained in the PNR will be sent to Secure Flight through a network connection provided by DHS's CBP. Reservations or changes to reservations that are made less than 72 hours prior to flight time will be sent immediately to TSA through CBP.

Upon receipt of passenger data, TSA plans to process the passenger data through the Secure Flight application running on the TVP. During this process, Secure Flight is to determine if the passenger data match the data extracted daily from TSC's Terrorist Screening Database (TSDB)—the information consolidated by TSC from terrorist watch lists to provide government screeners with a unified set of terrorist-related information. In addition, TSA will screen against its own watch list composed of individuals who do not have a nexus to terrorism but who may pose a threat to aviation security.[10]

In order to match passenger data to information contained in the TSDB, TSC plans to provide TSA with an extract of the TSDB for use in Secure Flight, and provide updates as they occur. This TSDB subset will include all individuals classified as either selectees (individuals who are selected for additional security measures prior to boarding an aircraft) or no-flys (individuals who will be denied boarding unless they are cleared by law enforcement personnel).[11] To perform the match, Secure Flight is to compare the passenger, TSDB, and other watch list data using automated name-matching technologies. When a possible match is generated, TSA and potentially TSC analysts will conduct a manual review comparing additional law enforcement and other government information with passenger data to determine if the person can be ruled out as a possible match. TSA is to return the matching results to the air carriers through CBP. Figure 1 illustrates how Secure Flight is intended to operate.

Figure 1: Planned Operation of Secure Flight



Source: GAO analysis of TSA data.

a. Information about confirmed no-flies and certain selectees are shared with appropriate Federal agencies which coordinate the appropriate law enforcement response.

As shown in figure 1, when the passenger checks in for the flight at the airport, the passenger is to receive a level of screening based on his or her designated category. A cleared passenger is to be provided a boarding pass and allowed to proceed to the screening checkpoint in the normal manner. A selectee passenger is to receive additional security scrutiny at the screening checkpoint.[12] A no-fly passenger will not be issued a boarding pass. Instead, appropriate law enforcement agencies will be notified. Law enforcement officials will determine whether the individual will be allowed to proceed through the screening checkpoint or if other actions are warranted, such as additional questioning of the passenger or taking the passenger into custody.

TSA Has Not Followed a Disciplined Life Cycle Approach or Fully Defined System Requirements, Schedule, and Costs

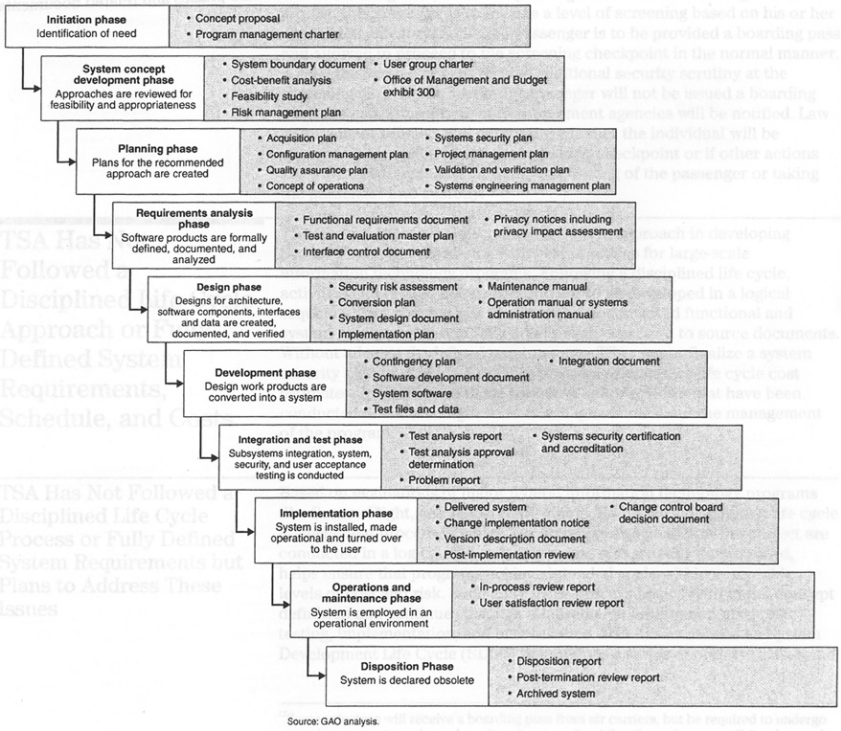
TSA has not followed a disciplined life cycle approach in developing Secure Flight, in accordance with best practices for large-scale information technology programs. Following a disciplined life cycle, activities and related documentation are to be developed in a logical sequence. TSA also has not finalized and documented functional and system requirements that fully link to each other and to source documents. Without adequately defined requirements, TSA cannot finalize a system security plan or develop a reliable program schedule or life cycle cost estimates. In addition to these concerns, other reviews that have been conducted of Secure Flight have raised questions about the management of the program.

TSA Has Not Followed a Disciplined Life Cycle Process or Fully Defined System Requirements but Plans to Address These Issues

Based on evaluations of major Federal information technology programs like Secure Flight, and research by others, following a disciplined life cycle management process in which key activities and phases of the project are conducted in a logical

and orderly process and are fully documented, helps ensure that programs achieve intended goals within acceptable levels of cost and risk. Such a life cycle process begins with initial concept definition and continues through requirements determination to final testing, implementation, and maintenance. TSA has established a System Development Life Cycle (SDLC) that defines a series of orderly phases and associated steps and documentation. The SDLC serves as the mechanism to ensure that systems are effectively managed and overseen. Figure 2 provides a description of TSA's SDLC phases and related documentation.

Figure 2: Summary of TSA's System Development Life Cycle Process



Source: GAO analysis.

TSA has not followed its SDLC in developing and managing Secure Flight. Rather, program officials stated that they have used a rapid development method that was intended to enable them to develop the program more quickly. However, these officials could not provide us with details on how this approach was implemented. As a result, our analysis of steps performed and documentation developed indicates that Secure Flight has not been pursued within the context of a logical, disciplined, system development methodology. Rather the process has been ad hoc, with project activities conducted out of sequence. For example, program officials declared that the program's design phase was completed before system requirements had been adequately detailed, and key activities have yet to be adequately performed, such as program planning and defining system requirements. TSA officials acknowledged that problems arose with Secure Flight as a result of using this approach. As a result, it is currently unclear what Secure Flight capabilities are to be developed, by when, at what cost, and what benefits are to accrue from the program. Without clarification on these decision points, the program is at risk of failure.

Defining and documenting system requirements is integral to life cycle development. Based on best practices and our prior work in this area, the expected capabilities of a system such as Secure Flight should be defined in terms of requirements for functionality (what the system is to do), performance (how well the system is to execute functions), data (what data are needed by what functions, when, and in what form), interface (what interactions with related and dependent systems are

needed), and security. Further, system requirements should be unambiguous, consistent with one another, linked (that is, traceable from one source level to another),[13] verifiable, understood by stakeholders, and fully documented.

TSA has prepared certain Secure Flight requirements documents, and officials stated that they are now reviewing those requirements documents.[14] We support these review efforts because we found, in the requirements documents we reviewed, inconsistencies and ambiguities in requirements documentation for system functions, performance, data, and security—and that these documents were not always complete. For example, according to TSA's SDLC guidance and best practices for developing information technology systems, systems like Secure Flight should have a comprehensive concept of operations covering all aspects of the program during the planning phase (see fig. 2). We reported in our March 2005 report that TSA had not yet finalized a concept of operations, which would describe conceptually the full range of Secure Flight operations and interfaces with other systems, and we recommended that it develop one. Since March 2005, TSA documents refer to numerous concept of operations, such as a long concept of operations, a short concept of operations, and an initial operational capability concept of operations. TSA provided a June 2005 concept of operations for our review, but this document does not contain key system requirements, such as the high-level requirements for security and privacy.

In addition, we found that Secure Flight requirements were unclear or missing. For example, while the requirements that we reviewed state that the system be available 99 percent of the time, this only covers the TVP and Secure Flight application. It does not include requirements for the interfacing systems critical for Secure Flight operations. Thus, the availability requirements for all of the components of the Secure Flight system are not yet known. Some data requirements are also vague or incomplete; for example, one data requirement is that the data is current, but the meaning of current is not defined. In addition, only some system security requirements are identified in the security document provided to us for the TVP, and sections in TSA's Systems Requirements Specification contain only placeholder notes—"to be finalized"—for security and privacy requirements.

TSA officials acknowledged that it is important that requirements be traceable to ensure that they are consistently, completely, and correctly defined, implemented, and tested. To help accomplish this, TSA officials stated that they use a requirements tracking tool for Secure Flight that can align related requirements to different documents, and thus establish traceability (e.g., it can map the Systems Requirements Specification to a functional requirements document). According to program officials, this tool can also be used for aligning and tracing requirements to test cases (i.e., scenarios used to determine that the system is working as intended). We found, however, that requirements for Secure Flight have not been fully traced. For example, we were not able to trace system capabilities in contractual documents to the concept of operations and then to the various requirement documents, to design phase use cases, and to test cases. In addition, contractor staff we interviewed stated that they were unable to use this tool to align or trace necessary requirements without the aid of supplemental information. Without internal alignment among system documentation relating to requirements, there is not adequate assurance that the system produced will perform as intended.

In addition, we found that available Secure Flight requirements documents did not define the system's boundaries, including interfaces, for each of the stakeholders—that is, the scope of the system from end to end, from an air carrier to CBP, to TSA, to TSC, and back to TSA, then again to CBP and air carriers (refer to fig. 1 for an overview of this process). Defining a system's boundaries is important in ensuring that system requirements reflect all of the processes that must be executed to achieve a system's intended purpose. According to TSA's SDLC guidance, a System Boundary Document is to be developed early in the system life cycle. However, in its third year of developing a passenger prescreening system, TSA has not yet prepared such a document. Although the System Boundary Document was not available, the program's Systems Security Document does refer to an "accreditation boundary," which defines the Secure Flight system from the standpoint of system security accreditation and certification. According to this definition of what Secure Flight includes, those systems that are needed to accomplish Secure Flight program goals (e.g., those of commercial air carriers, CBP, and TSC) are not part of Secure Flight. If the boundary documents, and thus the requirements, do not reflect all system processes and connections that need to be performed, the risk is increased that the system will not achieve Secure Flight's intended purpose. Moreover, until all system requirements have been defined, TSA will not be able to stress-test Secure Flight in an operational, end-to-end mode. In our March 2005 report, we recommended that TSA finalize its system requirements documents and ensure that

these documents address all system functionality. Although TSA agreed with our recommendations, the requirements documentation that we reviewed showed that the agency has not yet completed these activities.

Our evaluations of major Federal information technology programs, and research by others, has shown that following a disciplined life cycle management process decreases the risks associated with acquiring systems. The steps and products in the life cycle process each have important purposes, and they have inherent dependencies among themselves. Thus, if earlier steps and products are omitted or deficient, later steps and products will be affected, resulting in costly and time-consuming rework. For example, a system can be effectively tested to determine whether it meets requirements only if these requirements have already been fully defined. Concurrent, incomplete, and omitted activities in life cycle management exacerbate the program risks. Life cycle management weaknesses become even more critical as the program continues, because the size and complexity of the program will likely only increase, and the later problems are found, the harder and more costly they will likely be to fix.

In October 2005, Secure Flight's director of development stated in a memorandum to the assistant TSA administrator responsible for Secure Flight that by not following a disciplined life cycle approach, in order to expedite the delivery of Secure Flight, the government had taken a calculated risk during the requirements definition, design, and development phases of the program's life cycle development. The director stated that by prioritizing delivery of the system by a specified date in lieu of delivering complete documentation, TSA had to lower its standards of what constituted acceptable engineering processes and documentation. Since then, TSA officials stated that the required system documentation associated with each phase of the TSA life cycle is now being developed to catch up with development efforts. In addition, TSA recognized that it faces challenges preparing required systems documentation, and to help in this regard it has recently hired a certified systems program manager to manage systems development. In January 2006, this program manager stated that as Secure Flight moves forward, TSA's SDLC would be followed in order to instill greater rigor and discipline into the system's development. In addition, TSA plans to hire a dedicated program director for Secure Flight to manage program activities, schedules, milestones, costs, and program contractors, among other things.

Comprehensive System Security Management Program Has Not Yet Been Established in Accordance with Federal Guidance

TSA has taken steps to implement an information system security management program for protecting Secure Flight information and assets. Secure Flight's security plans and the related security review, which TSA developed and conducted to establish authority to operate, are important steps in the system's development. However, the steps related to system security TSA has taken to date are individually incomplete, and collectively fall short of a comprehensive system security management program. Federal guidance and industry best practices describe critical elements of a comprehensive information system security management program. Without effective system security management, it is unlikely that Secure Flight will, for example, be adequately protected against unauthorized access and use, disruption, modification, and destruction.

According to National Institute of Standards and Technology (NIST) [15] and Office of Management and Budget (OMB) guidance under the Federal Information Security Management Act, as well as industry best practices, a comprehensive system security management program includes (1) conducting a system wide risk assessment that is based on system threats and vulnerabilities, (2) developing system security requirements and related policies and procedures that govern the operation and use of the system and address identified risks, (3) certifying that the system is secure based on sufficient review and testing to demonstrate that the system meets security requirements, and (4) accrediting the system as secure in an operational setting.

TSA has developed two system security plans—one for the TVP and one for the Secure Flight application. However, neither of these plans nor the security activities that TSA has conducted to date are complete. For example, while security threats and vulnerabilities were assessed in the documentation and risks were identified in risk assessments, requirements to address these risks were only partially defined in the security plan for the TVP, and they were not included at all in the plan for the Secure Flight application. In addition, the sections on security requirements and privacy requirements in the System Requirements Specification document read "to be finalized" with no further description.

Moreover, we also found that the security systems plans did not reflect the current level of risk designated for the program. For example, although the July 15, 2005, System Security Plan for the TVP arrived at an overall assessment of its exposure to risks as being "medium," an August 23, 2005, requirements document found that the security risk level for the TVP was "high." As a system moves from a medium to a high level of risk, the security requirements become more stringent. TSA has not provided us with an updated System Security Plan for the TVP that addressed this greater level of risk by including additional NIST requirements for a high-risk system. In addition, this TVP System Security Plan included only about 40 percent of the NIST requirements associated with a medium-risk system. Without addressing all NIST requirements, in addition to those required for a high-risk system, TSA may not have proper controls in place to protect sensitive information.

According to Federal guidance and requirements, the determination and approval of the readiness of a system to securely operate is accomplished via a certification and accreditation process. On September 30, 2005, the TSA assistant administrator responsible for Secure Flight formally granted authority, based on certification and accreditation results, for the TVP and the Secure Flight application to operate.[16] However, the team performing the certification found that TSA was unsure whether they tested all components of the security system for the TVP and the Secure Flight application, because TSA lacked an effective and comprehensive inventory system. Therefore the certification team could not determine whether its risk assessments were complete or accurate. This team also documented 62 security vulnerabilities for the Secure Flight application and 82 security vulnerabilities for the TVP. The certification team recommended authority to operate on the condition that corrective action or obtaining an exemption for the identified vulnerabilities would be taken within 90 days or the authority to operate would expire. TSA officials stated that these vulnerabilities had been addressed except for three that are being reviewed in a current security audit.

Program Management Plan and Supporting Schedules and Cost Estimates for Secure Flight Have Not Been Maintained

TSA has proceeded with Secure Flight development over the past year without a complete and up-to-date program management plan, and without associated cost and schedule estimates showing what work will be done by whom, at what cost, and when. A program management plan can be viewed as a central instrument for guiding program development. Among other things, the plan should include a breakout of the work activities and products that are to be conducted in order to deliver a mission capability to satisfy stated requirements and produce promised mission results. This information, in turn, provides the basis for determining the time frames and resources needed for accomplishing this work, including the basis for milestones, schedules, and cost estimates. TSA has not provided us with either the complete and up-to-date program management plan, or an estimated schedule and costs for Secure Flight. According to a TSA official, an updated program management plan is currently being developed and is about 90 percent complete.

In lieu of a program management plan with a schedule and milestones, TSA has periodically disclosed program milestones. However, the basis for and meaning of these milestones have not been made clear, and TSA's progress in meeting these milestones has not been measured and disclosed. TSA's SDLC and OMB[17] guidance require that programs like Secure Flight provide risk-adjusted schedule goals, including key milestones, and that programs demonstrate satisfactory progress toward achieving their stated performance goals. In March 2005, we reported that the milestone that TSA set for achieving initial operating capability for Secure Flight had slipped from April 2005 to August 2005. TSA officials stated that TSA revised this milestone to state that instead of achieving initial operating capability, it would begin operational testing. This new milestone subsequently slipped first to September 2005, then to November 2005. Since that time, the program has not yet begun operational testing or initial operations, and TSA has not yet produced an updated schedule identifying when program operations will begin or when other key milestones are to be achieved to guide program development and implementation. Further, while agency officials stated that they are now planning for operational testing of an unspecified capability, no milestone date has been set for doing so.

TSA officials stated that they have not maintained an updated program schedule for Secure Flight in part because the agency has not yet determined the rulemaking approach it will pursue for requiring commercial air carriers to submit certain passenger data needed to operate Secure Flight, among other things. Specifically, TSA officials stated that a schedule with key milestones, such as operational testing, cannot be set until after air carriers have responded to the rulemaking and provided their plans and schedules for participating in Secure Flight. The rulemaking has

been pending since the spring of 2005, and the rule remains in draft form and is under review, according to TSA officials. Once the rule has been issued, TSA officials stated that air carriers will be given time to respond with their plans and schedules. TSA officials further stated that until this occurs, and a decision is made as to how many air carriers will participate in a yet-to-be-defined initial phase of the program (they are expected to begin incrementally), a program schedule cannot be set.

Further, TSA has not yet established cost estimates for developing and deploying either an initial or a full operating capability for Secure Flight, and it has not developed a life-cycle cost estimate (estimated costs over the expected life of a program, including direct and indirect costs and costs of operation and maintenance). TSA also has not updated its expenditure plan—plans that generally identify near-term program expenditures—to reflect the cost impact of program delays, estimated costs associated with obtaining system connectivity with CBP, or estimated costs expected to be borne by air carriers. Program and life cycle cost estimates are critical components of sound program management for the development of any major investment. Developing cost estimates is also required by OMB guidance and can be important in making realistic decisions about developing a system. Expenditure plans are designed to provide lawmakers and other officials overseeing a program's development with a sufficient understanding of the system acquisition to permit effective oversight, and to allow for informed decision making about the use of appropriated funds.

In our March 2005 report, we recommended that TSA develop reliable life cycle cost estimates and expenditure plans for the Secure Flight program, in accordance with guidance issued by OMB, in order to provide program managers and oversight officials with the information needed to make informed decisions about program development and resource allocations. Although TSA agreed with our recommendation, it has not yet provided this information. TSA officials stated that developing program and life cycle cost estimates for Secure Flight is challenging because no similar programs exist from which to base cost estimates and because of the uncertainties surrounding Secure Flight requirements. Further, they stated that cost estimates cannot be accurately developed until after system testing is completed and policy decisions have been made regarding Secure Flight requirements and operations. Notwithstanding these statements, TSA officials stated that they are currently assessing program and life cycle costs as part of their rebaselining and that this new baseline will reflect updated cost, funding, scheduling, and other aspects of the program's development.

While we recognize that program unknowns introduce uncertainty into the program-planning process, including estimating tasks, time frames, and costs, uncertainty is a practical reality in planning all programs and is not a reason for not developing plans, including cost and schedule estimates, that reflect known and unknown aspects of the program. In program planning, assumptions need to be made and disclosed in the plans, along with the impact of the associated uncertainty on the plans and estimates. As more information becomes known over the life of the program, these plans should be updated to recognize and reflect the greater confidence in activities that can be expressed with estimates.

Program management plans and related schedules and cost estimates—based on well-defined requirements—are important in making realistic decisions about a system's development, and can alert an agency to growing schedule or cost problems and the need for mitigating actions. Moreover, best practices and related Federal guidance emphasize the need to ensure that programs and projects are implemented at acceptable costs and within reasonable and expected time frames. Investments such as Secure Flight are approved on the expectation that programs and projects will meet certain commitments to produce certain capabilities and benefits (mission value) within the defined schedule and cost. Until an updated program management plan and related schedules and cost estimates and expenditure plans, are prepared for Secure Flight—which should be developed despite program uncertainties, and updated as more information is gained—TSA and Congress will not be able to provide complete oversight over the program's progress in meeting established commitments.

Oversight Reviews of Secure Flight Have Been Conducted and Raised Questions about Program Management

DHS and TSA have executive and advisory oversight mechanisms in place to oversee Secure Flight. As we reported in March 2005, the DHS Investment Review Board (IRB)—designed to review certain programs at key phases of development to help ensure they meet mission needs at expected levels of costs and risks—reviewed the TVP from which Secure Flight will operate, in January 2005.[18] As a result of

this review, the board withheld approval for the TVP to proceed from development and testing into production and deployment until a formal acquisition plan, a plan for integrating and coordinating Secure Flight with other DHS people-screening programs, and a revised acquisition program baseline (cost, schedule, and performance parameters) had been completed. Since that time, TSA has not yet addressed these conditions and has not obtained approval from the IRB to proceed into production. DHS officials stated that an IRB review is scheduled to be held in March 2006—14 months after the IRB last met to examine Secure Flight—to review Secure Flight and other people-screening programs, including international prescreening conducted by CBP. Specifically, the board will review the acquisition strategy and progress for each program, focusing, in part, on areas of potential duplication. According to TSA officials, the agency intends to establish a new program cost, schedule, and capability baseline for Secure Flight, which will be provided to the IRB for review.

DHS's Data Privacy and Integrity Advisory Committee also reviewed Secure Flight during the last year.[19] Committee Members have diverse expertise in privacy, security, and emerging technology, and come from large and small companies, the academic community, and the nonprofit sector. In December 2005, the committee issued five recommendations on key aspects of the program, including recommendations designed to minimize data collection and provide an effective redress mechanism to passengers who believe they have been incorrectly identified for additional security scrutiny. TSA officials stated that they are considering the advisory committees' findings and recommendations as part of their rebaselining efforts.

In September 2004, TSA appointed an independent working group within the Aviation Security Advisory Committee,[20] composed of government privacy and security experts, to review Secure Flight. The working group issued a report in September 2005 that concluded, among other things, that TSA had not produced a comprehensive policy document for Secure Flight that could define oversight or governance responsibilities, nor had it provided an accountability structure for the program. The group attributed this omission to the lack of a program-level policy document issued by a senior executive, which would clearly state program goals. The working group also questioned Secure Flight's oversight structure and stated that it should focus on the effectiveness of privacy aspects of the program and, in doing so, consider oversight regimes for Federal law enforcement and U.S. intelligence activities.

In addition to oversight reviews initiated by DHS and TSA, the DOJ–OIG issued a report in August 2005 reviewing TSC's role in supporting Secure Flight.[21] In its report, the DOJ–OIG reported that TSC faced several key factors that were unknown with respect to supporting Secure Flight, including when the program will begin, the volume of inquiries it will receive, the number of TSC resources required to respond to these inquiries, and the quality of the data it will have to analyze. In light of these findings, the DOJ–OIG report recommended that, among other things, TSC better prepare itself for future needs related to Secure Flight by strengthening its budgeting and staffing processes and by improving coordination with TSA on data exchange standards. In June 2005, a DOJ–OIG report recommended that TSC conduct a record-by-record review of the TSDB to improve overall data quality and integrity. TSC agreed with all recommendations made.[22]

TSA Has Made Progress in Coordinating With Critical Stakeholders but More Work Remains

TSA has drafted policy and technical guidance to help inform air carriers of their Secure Flight responsibilities, and has begun coordinating with CBP and TSC on Secure Flight requirements and broader issues of integration and interoperability between Secure Flight and other people-screening programs. However, TSA has not yet provided information and technical requirements that all stakeholders need to finalize their plans to support the program's operations, and to adequately plan for the resources needed to do so.

TSA Has Begun Collaborating With Key Stakeholders, but Their Participation Will Be Limited Until System Requirements Have Been Finalized

As we reported in March 2005, key Federal and commercial stakeholders—CBP, TSC, and commercial air carriers—will play a critical role in the collection and transmission of data needed for Secure Flight to operate successfully. Accordingly, TSA will need to ensure that requirements for each stakeholder are determined. For instance, TSA will need to define how air carriers are to connect to CBP and what passenger data formats and structures will be used. Although more remains to be done, TSA has worked to communicate and coordinate requirements with stake-

holders. For example, TSA has maintained weekly communications with CBP and TSC regarding their roles and responsibilities related to Secure Flight operations.

TSA has also begun to address air carriers' questions about forthcoming Secure Flight requirements. For example, TSA Officials have produced draft air carrier guidance, known as the Secure Flight Data Transmission Plan Guidance (DTPG).[23] The final DTPG is to include guidance to air carriers addressing the following areas: Secure Flight's mission overview and objectives, project planning phases, aircraft operator operations and airport procedures, technical data requirements, aircraft operator application development, Secure Flight operations, and system maintenance and support. According to TSA officials, air carriers have received copies of a partial draft DTPG, and some air carriers have submitted feedback to Secure Flight's Airline Implementation and Operations Team that TSA says it is working to address.

In addition to drafting guidance, TSA has conducted preliminary network connectivity testing between TSA and Federal stakeholders. For example, messages have been transmitted from CBP to TSA and back. However, such tests included only dummy data. According to CBP officials, no real-time passenger data have been used in this testing, and system stress testing has not yet been conducted.[24] Without real-time passenger data, the official said, CBP cannot estimate total capacity or conduct stress testing to ensure the system operates effectively. Further, according to a TSC official, testing has been conducted to show that a data exchange between the TSC and TSA is functioning, but the system has not been stress-tested to determine if it can handle the volume of data traffic that will be required to operate Secure Flight. According to this official, TSA has not specified what these data volume requirements will be. TSA officials acknowledged that they have not yet made this determination and stated that they will not be able to do so until they (1) issue the rule, and (2) have received the air carrier plans for participating in Secure Flight based on requirements identified in the rule.

Although CBP, TSC, and air carrier officials we interviewed acknowledged TSA's outreach efforts, they cited several areas where additional information was needed from TSA before they could fully support Secure Flight. Several CBP officials stated, for example, that they cannot proceed with establishing connectivity with all air carriers until DHS publishes the rule—the regulation that will specify what type of information is to be provided for Secure Flight—and the air carriers provide their plans for providing this information. Similarly, a TSC official stated that TSC cannot make key decisions on how to support Secure Flight until TSA provides estimates of the volume of potential name matches that TSC will be required to screen, as identified above. The TSC official stated that without this information, TSC cannot make decisions about required resources, such as personnel needed to operate its call center.[25] As we reported in March 2005, air carriers also expressed concerns regarding the uncertainty of the Secure Flight system and data requirements, and the impact these requirements may have on the airline industry and traveling public. Air carriers will not be able to begin to modify their passenger data systems to record the data attributes—such as full name and date of birth, which Secure Flight will use to conduct name matching—until TSA determines and communicates which specific data attributes are to be used.

Oversight groups that have reviewed Secure Flight agreed that additional work was needed to improve the flow of information to, and coordination with, program stakeholders. In its December 2005 report on Secure Flight, the DHS Data Privacy and Integrity Advisory Committee stated that TSA needs to be clear with air carriers about what information it needs now and what information it may consider requesting in the future, to enable air carriers to avoid sequential revisions of data-handling systems. Also, in September 2005, the Aviation Security Advisory Committee working group expressed concerns about the lack of clarity regarding how Secure Flight will interact with other screening programs.

Further, in its August 2005 audit of TSC's support of Secure Flight, the DOJ–OIG reported that TSC officials believed that their ability to prepare for the implementation of Secure Flight has been hampered by TSA's failure to make, communicate, and comply with key program and policy decisions in a timely manner, such as the launch date and volume of screening to be conducted during initial implementation. In addition, the report noted that because TSA is unsure about how many air carriers will participate in the initial phase of the program, neither TSA nor TSC can know how many passenger records will be screened, and cannot project the number of watch list hits that will be forwarded to the TSC for action. Finally, the DOJ–OIG report concluded that the shifting of critical milestones—including TSA's schedule slippages over the past year—has affected TSC's ability to adequately plan for its role in Secure Flight.

Despite TSA's outreach efforts, stakeholder participation in Secure Flight is dependent on TSA's effort to complete its definition of requirements and describe these

in the rule. Because TSA has not fully defined system requirements, key stakeholders have not been able to fully plan for or make needed adjustments to their systems. In our March 2005 report, we recommended that TSA develop a plan for establishing connectivity among the air carriers, CBP, and TSC to help ensure the secure, effective, and timely transmission of data for use in Secure Flight operations. Although TSA has continued to coordinate with these key stakeholders, at present the agency has still not completed the plans and agreements necessary to ensure the effective support of Secure Flight.

Ongoing Coordination of Prescreening and Name-Matching Initiatives Can Impact How Secure Flight Is Implemented

In January 2006, TSA officials stated that they are in the early stages of coordinating with CBP on broader issues of integration and interoperability related to other people-screening programs. These broader coordination efforts, which are focused on minimizing duplicative efforts that may exist between the agencies that screen individuals using watch list data and achieving synergies and efficiencies, are important because they may affect how Secure Flight will operate initially and in the future. Specifically, TSA Officials stated that they are coordinating more closely with CBP's international prescreening initiatives for passengers on flights bound for the United States. The Air Transport Association and the Association of European Airlines—organizations representing air carriers—had requested, among other things, that both domestic and international prescreening function through coordinated information connections and avoid unnecessary duplication of communications, programming, and information requirements. [26]

In response to air carrier concerns, and the initiatives of DHS to minimize duplicative efforts, officials from both CBP and TSA explained that they are beginning to work together to ensure that air carriers have a single interface with the government for prescreening both domestic and international passengers. TSA and CBP officials further stated that they will try to use CBP's network to transmit domestic and international passenger data to and from the air carriers, thus providing the air carriers with a single interface for sending and receiving information. [27] TSA and CBP officials also stated that air carriers should receive a common notification about whether a passenger—domestic or international—requires normal processing, additional screening, or is not permitted to board a plane. However, according to these officials, TSA and CBP have not yet resolved other system differences—such as the fact that their prescreening systems use different passenger data elements, documentation, [28] and name matching technologies—that could lead to conflicting notifications that would instruct air carriers to handle a passenger differently for an international than for a domestic flight. Both TSA and CBP officials agreed that additional coordination efforts are needed to resolve these differences, and stated that they plan to work closely together in developing a prescreening capability for both domestic and international passengers. [29] Decisions made as a result of further coordination could result in changes to the way that Secure Flight is implemented.

In addition to coordinating with CBP on international prescreening, TSA faces additional coordination challenges working with TSC. Specifically, according to TSC officials, TSC has an initiative under way to, among other things, better safeguard watch list data. Currently, TSC exports watch list data to other Federal agencies, such as TSA and the State Department, for use in these agencies' screening efforts or processes for examining documents and records related to terrorism. However, TSC is currently developing a new system whereby watch list data would not be exported, but rather would be maintained by TSC. This system, called Query, is to serve as a common shared service that will allow agencies to directly search the TSDB using TSC's name matching technology for their own purposes. TSC has conducted limited testing of the system. If TSC chooses to use Query, TSA will be required to modify the system architecture for Secure Flight in order to accommodate the new system. According to a TSC official, this effort could be costly. While TSA acknowledged in its draft concept of operations plan in June 2005 that Secure Flight would need to be modified to accommodate TSC's Query "as necessary," the agency has not made adjustments to its system requirements or conducted a cost analysis of expected impacts on the Secure Flight program. Rather, TSA has decided that it will continue developing the Secure Flight application, which includes TSA's name-matching technologies. Thus, TSC will need to export watch list data to TSA to support Secure Flight, once it becomes operational.

Key Factors That Will Influence the Effectiveness of Secure Flight Have Not Been Finalized or Resolved

Several activities are under way, or are to be decided, that will affect Secure Flight's effectiveness, including how operational testing is conducted, and how data

requirements and data accuracy are determined. TSA has been testing and evaluating name-matching technologies for determining what type of passenger data will be needed to match against the TSDB. These tests have been conducted thus far in a controlled, rather than real-world environment, using historical data, and additional testing is needed. In addition, TSA has not made key decisions regarding how the name-matching technologies to be used by Secure Flight will operate or which data will be used to conduct name matching. While TSA is not responsible for ensuring the accuracy of passenger data, the agency must nonetheless advise stakeholders on data accuracy and quality requirements. Another factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system's inability to identify passengers who assume the identity of another individual by committing identity theft, or passengers who use false identifying information. Secure Flight is neither intended to nor designed to address these vulnerabilities.

Tests of Name-Matching Capability Are Under Way, but Full System Testing Has Not Yet Been Conducted

TSA has tested—and continues to test—the effectiveness of one aspect of the Secure Flight system, namely name-matching technologies. These name-matching tests will help TSA determine what passenger data will be needed for the system to match most effectively passenger records with information contained in the TSDB. These tests are critical to defining data requirements and making decisions about how to configure the name-matching technologies. Additional tests will need to be conducted in an operational, real-world environment to fully understand how to configure the system effectively. This is because the name-matching tests conducted to date were conducted in a controlled, rather than real-world, environment—that is, under controlled, or simulated, conditions. For example, TSA used historic air carrier passenger data from June 2004 and historic and simulated watch list data to test the functionality and effectiveness of Secure Flight's name-matching technologies that match air carrier passenger records with potential terrorists in the TSDB.

Additional testing beyond name-matching also needs to be conducted, after TSA rebaselines its program, defines system requirements, and begins adhering to its SDLC. For example, stress and operational testing [30] would help determine whether Secure Flight can process the volume of data expected and operate as intended in an operational environment. As we reported in March 2005, TSA had planned to conduct a series of operational tests consisting of increasingly larger increments of the system's functionality until the complete system was tested. These tests were to begin in June 2005. However, due to program delays, TSA has not yet conducted this end-to-end testing needed to verify that the entire system, including any interfaces with external systems, functions as intended in an operational environment. TSA also has not yet conducted the stress testing needed to measure the system's performance and availability in times of particularly heavy (i.e., peak) loads. Recently, TSA documented its overall strategy for conducting these tests and developed draft test plans. TSA officials stated that information about its plans for future testing will be included in its rebaselined program plan. Until this testing is complete, it will not be possible to determine whether Secure Flight will function as intended in an operational environment.

Key Policy Decisions That Will Impact System Effectiveness Have Not Been Made

Key policy decisions that will influence the effectiveness of Secure Flight in identifying passengers who should undergo additional security scrutiny have not yet been made. These policy decisions include (1) determining the passenger information that air carriers will be required to collect and provide for vetting, (2) the name-matching technologies that will be used to vet passenger data against data contained in the TSDB, and (3) the thresholds that will be set to determine when a passenger will be identified as a potential match against the TSDB. These three decisions, discussed below, are all critical to ensuring that Secure Flight identifies potential terrorist threats as effectively as possible while minimizing the number of potential matches that will require further review by TSA and TSC analysts.

(1) Determining the passenger information that air carriers will be required to collect and provide for vetting: TSA needs to decide which data attributes air carriers will be required to provide in passenger data to be used to match against data contained in the TSDB, such as full first, middle, and last name plus other discrete identifiers, such as date of birth.

Using too many data attributes can increase the difficulty of matching, since the risk of errors or mismatches increases. Using too few attributes can create an unnecessarily high number of incorrect matches due to, among other things, the dif-

ficulty of differentiating among similar common names without using further information. Initial TSA test results have shown that the use of name and date of birth alone might not be sufficient for decreasing the number of false positives—that is, passengers inappropriately matched against data contained in the TSDB.

(2) Selecting name-matching technologies used to vet passenger names against the TSDB: TSA must determine what type or combination of name-matching technologies to acquire and implement for Secure Flight, as these different technologies have different capabilities. For example, TSA's PNR testing showed that some name-matching technologies are more capable than others at detecting significant name modifications, which allows for the matching of two names that contain some variation. Detecting variation is important because passengers may intentionally make alterations to their names in an attempt to conceal their identity. Also, unintentional variations can result from different translations of nonnative names or data entry errors. For example, some name-matching technologies might correctly discriminate between "John Smith" and "John Smythe," others may not. However, name matching technologies that are best at detecting name variations may also increase the number of potential matches that will have to be further reviewed, which could be offset using a combination of name matching technologies. TSA officials stated in November 2005 that it planned to continuously evaluate the best name-matching technologies or combination of technologies to enhance the system in future iterations. TSA officials recently stated that they had made, but not yet documented, an initial determination regarding the name-matching technologies that will be used for Secure Flight and that they plan to conduct continuous reviews of the name-matching technologies to address circumstances as they arise.

(3) Selecting thresholds for determining when a possible name match has occurred: TSA has discretion to determine what constitutes a possible match between a passenger's data and a TSDB record.[31] For each name that is matched, the name-matching tool will assign a numeric score that indicates the strength of the potential match.[32] For example, a score of 95 out of 100 would indicate a more likely match than a score of 85. If TSA were to set the threshold too high, many names may be cleared and relatively few flagged as possible matches—that is, there is a possibility that terrorists' names may not be matched. Conversely, if the threshold were set too low, passengers may be flagged unnecessarily, and relatively few cleared through the automated process. As an example of the importance of setting thresholds, during one of the PNR tests conducted, TSA set the name-matching threshold at 80, which resulted in over 60 percent of passengers requiring manual review. Alternatively, when TSA set the threshold at 95, less than 5 percent of the same group of passenger records were identified as requiring further review. With about 1.8 million passengers traveling domestically per day, having a threshold that is too low could produce an unmanageable number of matches—possibly leading to passenger delays—while setting the threshold too high could result in the system missing potential terrorists. Although TSA will not decide how the thresholds should be set until it conducts additional evaluations, it has indicated that the threshold might be adjusted to reflect changes in the terrorist threat level. This would result in Secure Flight flagging more names for potential manual review in order to ensure greater scrutiny in response to changing conditions.

TSA plans to finalize decisions on these factors as system development progresses. However, until these decisions are made, requirements will remain unsettled and key stakeholders—in particular air carriers—will not have the information they need to assess and plan for changes to their systems necessary for interfacing with Secure Flight. Air carriers and reservation companies will also not know which additional data attributes they may be required to collect from passengers, to support Secure Flight operations, as reservations are made. These decisions will also directly influence the number of analysts that TSA and TSC will need to manually review potential matches to the TSDB. Accordingly, stakeholders have expressed concern that they have not been provided information about what these decisions are. They stated that they are awaiting additional information from TSA in order to move forward with their plans to interface with and support Secure Flight.

Efforts to Improve Data Quality and Accuracy Are Under Way, but Additional Work Remains

Two additional factors that will impact the effectiveness of Secure Flight are (1) the accuracy and completeness of data contained in TSC's TSDB and in passenger data submitted by air carriers, and (2) the ability of TSA and TSC to identify false positives and resolve possible mistakes during the data matching process, in order to minimize inconveniencing passengers. According to TSA and TSC officials, the data attributes that Secure Flight will require for name matching need to be included in both the passenger data and the TSDB in order for the automated system

to effectively match names between the two lists. As we reported in March 2005, while the completeness and accuracy of data contained in the TSDB can never be certain—given the varying quality of intelligence information gathered, and changes in this information over time—TSC has established some processes to help ensure the quality of these data. However, the DOJ–OIG, in its June 2005 review of TSC,[33] found that the TSC could not ensure that the information contained in its databases was complete or accurate.[34] According to a TSC official, since the time of the DOJ–OIG review, TSC has taken several steps to improve the quality of TSDB records, including conducting a record-by-record review, updating procedures for a daily review of each new or modified record, and using automated rules to check the completeness of records received from other agencies.[35] According to this official, TSA and TSC plan to enter into a letter of agreement that will describe the TSDB data elements that TSC will produce for TSA, among other things, to be used for Secure Flight. However, these data requirements have not yet been determined.

In order to obtain accurate and complete passenger data from air carriers, TSA plans to describe the required data attributes that must be contained in passenger data provided to TSA in the forthcoming rule. TSA also plans to issue a final and complete DTPG to specify the data formats and other transmission requirements. However, the accuracy and completeness of the information contained in the passenger data record will still be dependent on the air carriers' reservations systems and passengers, and the air carriers' modifications of their systems for transmitting the data in the proper format. These steps are not trivial, as indicated by the June 2004 historical passenger data provided by the air carriers for TSA's name-matching tests. For these tests, many passenger data records submitted by air carriers were found to be inaccurate or incomplete, creating problems during the automated name-matching process. For example, some passenger data included invalid characters or prefixes, such as "Mr." and "Mrs.," in the name fields. Other inaccuracies included invalid characters or prefixes, spelling errors, and inverted birth date information. Additionally, some of the records had omitted or incomplete data elements necessary for performing the automated match or were in an unusable format.

In a related effort to address accuracy, TSA and TSC plan to work together to identify false positives as passenger data are matched against data in the TSDB and to resolve mistakes to the extent possible before inconveniencing passengers. The agencies will use intelligence analysts during the actual matching of passenger data to data contained in the TSDB to increase the accuracy of data matches. As indicated in figure 1, when TSA's name-matching technologies indicate a possible match, TSA analysts are to manually review all of the passenger data and other information to determine if the passenger can be ruled out as a match to the TSDB. If a TSA analyst cannot rule out a possible match, the record will be forwarded to a TSC analyst to conduct a further review using additional information. According to a TSC official, TSA and TSC analysts participated in a tabletop exercises to test the consistency of their respective manual reviews, and found that the matching logic used by both groups of analysts was consistent. This official stated that TSA and TSC also tested their operational procedures, and found gaps in their procedures that are now being addressed. According to this official, TSA and TSC plan to conduct additional joint exercises. Completing these exercises will be important to further understanding the effectiveness of using intelligence analysts to clear misidentified passengers during Secure Flight operations.

False Identifying Information and Identity Theft Could Impact the Security Benefits of Secure Flight

Another factor that could affect Secure Flight's effectiveness in identifying known or suspected terrorists is the system's inability to identify passengers who falsify their identifying information or who commit identity theft.[36] TSA Officials stated that the program is not intended to or designed to protect against the use of falsified identities or to detect identity theft. However, TSA officials stated that the use of commercial data during the name-matching process may help identify situations in which a passenger submits fictitious information such as a false address. In the spring of 2005, a TSA contractor tested the use of commercial data composed of personally identifiable information (such as name and address) to determine, among other things, if such data could be used to increase Secure Flight's effectiveness in identifying false or stolen identities. However, according to the DHS Data Privacy and Integrity Advisory Committee report, testing performed to date does not provide a reasonable case for utilizing commercial data as part of Secure Flight. TSA officials are not currently pursuing the use of commercial data to support Secure Flight because the Fiscal Year 2006 DHS Appropriations Act prohibits TSA from using data or databases obtained from or that remain under the control of a non-federal entity,[37] effectively terminating this type of testing for the duration of Fiscal Year

2006.[38] Further, TSA officials stated that incorporating biometrics—technologies that can automate the identification of people by one or more of their distinct physical or behavioral characteristics—is not currently envisioned for Secure Flight. As noted in our previous work, biometric technologies, such as fingerprint recognition, are being used in other TSA screening programs.[39] Moreover, the current prescreening process of matching passenger names against no-fly and selectee lists implemented by air carriers also does not protect against identity theft or the use of fictitious identities.

Secure Flight Privacy Notices and Passenger Redress Process Cannot Be Finalized Until Program Requirements Are More Fully Defined

TSA is aware of, and plans to address, the potential for Secure Flight to adversely affect travelers' privacy and impact their rights. However, TSA, as part of its requirements development process, has not yet clearly identified the privacy impacts of the planned system or the full actions it plans to take to mitigate them. Nor has the agency completed its assessment of the potential impact on passenger privacy of the system in an operational environment or defined its redress process for Secure Flight because, in part, the operational plans and system requirements for Secure Flight have not been finalized. TSA officials stated that they are in the process of reviewing new privacy notices that will be issued in conjunction with a forthcoming rule making prior to proceeding with its initial operating capability, and that these notices will also address certain aspects of Secure Flight's redress process. Until TSA finalizes system requirements and notices, however, privacy protections and impacts cannot be assessed.

Privacy Cannot Be Fully Assessed Because System Development Documentation Does Not Fully Address Privacy Requirements

The Privacy Act and the Fair Information Practices—a set of internationally recognized privacy principles that underlie the Privacy Act—limit the collection, use, and disclosure of personal information by Federal agencies.[40] While TSA has reiterated its commitment to meet the requirements of the Privacy Act and the Fair Information Practices, it is not yet evident how this will be accomplished.[41] To begin with, TSA has not decided what data attributes from the PNR it plans to collect, or how such data will be provided by airlines, through CBP, to TSA. Further, according to TSA officials, the agency is in the process of developing but has not issued the system of records notice, which is required by the Privacy Act,[42] or the privacy impact assessment, which is required by the E-Government Act,[43] that would describe how TSA considered privacy in the development of the system and how it will protect passenger data once the system becomes operational.

Moreover, privacy requirements were not incorporated into the Secure Flight system development process in such a way that would explain whether personal information will be collected and maintained in the system in a manner that complies with statutory requirements and TSA's SDLC guidance. One requirement of the privacy impact assessment is that privacy be addressed in the systems development documentation. In addition, TSA's SDLC guidance acknowledges that privacy protections should be planned for and carried out as part of the system development process. In our review of Secure Flight's system requirements, we found that privacy concerns were broadly addressed in Secure Flight's functional requirements, but had not been translated into specific system requirements. For example, the functional requirements stated that the Privacy Act must be considered in the development of the system, but the system requirements documents do not reflect how privacy protections will be supported by the system. Rather, system requirements documents state that privacy requirements are "yet to be finalized." TSA's Privacy Officer stated that she has been collaborating with the system development team, but this is not evident in the documents we reviewed.

Without taking steps to ensure that privacy protections are built into the system requirements, TSA cannot be assured that it will be in compliance with the Privacy Act once operational, and it runs the risk of repeating problems it experienced last spring. We reported in July 2005 that TSA's initially issued privacy notices for the Secure Flight data-processing tests did not meet Privacy Act requirements because personal information was used in testing in ways that the agency had not disclosed to the public.[44] We explained that in its fall 2004 notices, TSA had informed the public of its plans to use personal information during Secure Flight testing, including the use of commercial data in a limited manner. However, these initial notices did not fully describe how personal information would be collected, used, and stored for commercial data testing as it was carried out. As a result, individuals were not fully informed that their personal information was being collected and used, nor did they have the opportunity to comment on this or become informed on how they

might exercise their rights of access to their information. Although TSA did not fully disclose its use of personal information prior to beginning Secure Flight commercial data testing, the agency issued revised privacy notices in June 2005 to more fully disclose the nature of the commercial tests and address the issues disclosed by us.

As we reported in March 2005, until TSA fully defines its operational plans for Secure Flight and addresses international privacy concerns, it will remain difficult to determine whether the planned system will offer reasonable privacy protections to passengers who are subject to prescreening or mitigate potential impacts on passengers' privacy. At that time, we recommended that TSA finalize privacy policies and issue associated documentation prior to Secure Flight achieving initial operating capability. TSA acknowledged that it needs to publish new privacy notices to cover the collection, use, and storage of personal data for Secure Flight's initial and full operating capability, before beginning operational testing. TSA officials stated that these privacy notices are currently being reviewed by TSA and DHS and will be released in conjunction with the forthcoming rulemaking.

TSA Has Not Determined Secure Flight's Redress Process

Congress mandates that Secure Flight include a process whereby aviation passengers determined to pose a threat to aviation security may appeal that determination and correct erroneous information contained within the prescreening system. [45] TSA currently has a process in place that allows passengers who experience delays, under the current process run by air carriers, to submit a passenger identity verification form to TSA and request that the agency place their names on a cleared list. If, upon review, TSA determines that the passenger's identity is distinct from the person on a watch list, TSA will add the passenger's name to its cleared list, and will forward the updated list to the air carriers. TSA will also notify the passenger of his or her cleared status and explain that in the future the passenger may still experience delays. [46] Recently, TSA has automated the cleared list process, enabling the agency to further mitigate inconvenience to travelers on the cleared list.

The Intelligence Reform and Terrorism Prevention Act, enacted in December 2004, directs TSA to include certain elements in its Secure Flight redress policy. [47] Specifically, it requires the establishment of a timely and fair process for individuals identified as a threat to appeal the determination to TSA and correct any erroneous information. [48] It further requires that TSA establish a method for maintaining a record of air passengers who have been misidentified and have corrected erroneous information. To prevent repeated delays of misidentified passengers, this record must contain information determined by TSA to authenticate the identity of such a passenger. In January 2006, TSA officials stated that no final decisions have been made regarding how TSA will address the relevant requirements for redress found in the Intelligence Reform and Terrorism Prevention Act requirements. However, OTSR officials stated that a cleared list will be part of the process. The June 2005 concept of operations describes a process where individuals that are frequently misidentified as being on the TSDB and TSA selectee list can request to be placed on a list of individuals who have been cleared.

In our March 2005 report, we recommended that TSA finalize its Secure Flight redress policies and procedures prior to achieving its initial operating capability. Information concerning aspects of the redress process will be published before operational tests or full implementation of the Secure Flight process, and will be contained within the privacy notices that TSA officials stated will be released in conjunction with the forthcoming rulemaking. Moving forward, TSA has assigned a manager to serve as liaison with DHS on privacy and redress issues.

Concluding Observations

TSA has continued its development and testing of Secure Flight, but has made limited progress in addressing longstanding issues related to system development and testing, program management, and privacy and redress protections. To make and demonstrate progress on any large-scale information technology program, such as Secure Flight, an agency must first adequately define what program capabilities, such as requirements related to performance, security, privacy, and data content and accuracy, are to be provided. These requirements can then in turn be used to produce reliable estimates of what these capabilities will cost, when they will be delivered, and what mission value or benefits will accrue as a result. For Secure Flight, well-defined requirements would provide a guide for developing the system and a baseline to test the developed system to ensure that it delivers necessary capabilities, and would help to ensure that key program areas—such as security, system connectivity, privacy and redress protections—are appropriately managed.

When we reported on Secure Flight in March 2005, TSA had committed to take action on our recommendations to manage the risks associated with developing and

implementing Secure Flight, including finalizing the concept of operations, system requirements and test plans; completing formal agreements with CBP and air carriers to obtain passenger data; developing life cycle cost estimates and a comprehensive set of critical performance measures; issuing new privacy notices; and putting a redress process in place. Over the past 11 months, TSA has made some progress on all of these areas, including conducting further testing of factors that could influence system effectiveness and corroborating with key stakeholders. However, TSA has not completed any of the actions it had scheduled to accomplish. In particular, TSA has not yet developed complete system requirements or conducted important system testing (including stress testing), fully established security measures, made key decisions that will determine system effectiveness, developed a program management plan and a schedule for accomplishing program goals, or published updated privacy and redress notices. Taken as a whole, this lack of progress indicates that the program has not been effectively managed and is at risk of failure.

While we recognize that TSA faces program uncertainties that can directly impact Secure Flight's development and progress, uncertainty is a component of most programs, and should not be used as a reason for not defining requirements and developing plans and cost estimates, to manage risk. We believe that Secure Flight, like all programs, can utilize best practices to develop such plans to manage program uncertainties.

To its credit, TSA has recently taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, including hiring a program manager with information systems program management credentials. We also support TSA's efforts to rebaseline the program, including defining system requirements and finalizing a program management plan, including the development of schedules and cost estimates, before proceeding with program development. In fact, proceeding with operational testing and completing other key program activities should not be pursued until TSA puts in place a more disciplined life cycle process and defines system requirements. In the absence of this and other program information, such as requirements, capabilities, and benefits, further investment in this program would be difficult to justify.

We are also encouraged that DHS's IRB—the executive decision making authorities—has scheduled a review of Secure Flight and other people-screening programs. Given the potential duplication with CBP's new initiatives for international prescreening, DHS, TSA, and CBP need to assess alternative system solutions that should be factored into Secure Flight's rebaselined program and be the basis for IRB decisions regarding Secure Flight's future. Notwithstanding these efforts, however, much work remains to be accomplished before Secure Flight is positioned to be properly executed so that informed and prudent investment decisions can be made.

Mr. Chairman, this concludes my prepared statement. I will be pleased to respond to any questions that you or other Members of the Committee have at the appropriate time.

GAO Contacts and Staff Acknowledgments

For further information about this testimony, please contact Cathleen Berrick, at 202–512–3404 or at *berrickc@gao.gov* or Randolph C. Hite at 202–512–6256 or at *hiter@gao.gov*.

Other key contributors to this statement were David Alexander, Amy Bernstein, Mona Nichols Blake, John de Ferrari, Christine Fossett, Brent Helt, Richard Hung, Thomas Lombardi, C. James Madar, Matthew Mohning, David Plocher, Karl Seifert, and William Wadsworth.

APPENDIX I

Legislatively Mandated Secure Flight Issues to be Certified by the DHS and Reviewed by GAO

Legislative mandated issue (number and short title)	Description of mandated issue
1. Redress process	A system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights by TSA may appeal such decisions and correct erroneous information contained in CAPPS II or Secure Flight or other follow-on/successor programs.

Legislatively Mandated Secure Flight Issues to be Certified by the DHS and Reviewed by GAO—Continued

Legislative mandated issue (number and short title)	Description of mandated issue
2. Accuracy of databases and effectiveness of Secure Flight	The underlying error rate of the government and private databases that will be used to both establish identity and assign a risk level to a passenger will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted.
3. Stress testing	TSA has stress-tested and demonstrated the efficacy and accuracy of all search technologies in CAPPS II or Secure Flight or other follow-on/successor programs and has demonstrated that CAPPS II or Secure Flight or other follow-on/successor programs can make an accurate predictive assessment of those passengers who may constitute a threat to aviation.
4. Internal oversight	The Secretary of Homeland Security has established an internal oversight board to monitor the manner in which CAPPS II or Secure Flight or other follow-on/successor programs are being developed and prepared.
5. Operational safeguards	TSA has built in sufficient operational safeguards to reduce the opportunities for abuse.
6. Security measures	Substantial security measures are in place to protect CAPPS II or Secure Flight or other follow-on/successor programs from unauthorized access by hackers or other intruders.
7. Oversight of system use and operation	TSA has adopted policies establishing effective oversight of the use and operation of the system.
8. Privacy concerns	There are no specific privacy concerns with the technological architecture of the system.
9. Modifications with respect to intrastate travel to accommodate states with unique air transportation needs	TSA has, in accordance with the requirements of section 44903 (j)(2)(B) of title 49, United States Code, modified CAPPS II or Secure Flight or other follow-on/successor programs with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger primary selectee status.
10. Life-cycle cost estimates and expenditure plans	Appropriate life-cycle cost estimates, and expenditure and program plans exist.

Source: GAO.

ENDNOTES

[1] Section 518 of the Department of Homeland Security Appropriations Act, 2006 (Pub. L. 109–90) requires GAO to report to the Committees on Appropriations of the Senate and House of Representatives on the 10 issues listed in § 522(a) the Department of Homeland Security Appropriations Act, 2005 (Pub. L. 108–334), not later than 90 days after the Secretary of the Department of Homeland Security certifies to the above-named committees that Secure Flight has satisfied the 10 issues. These 10 issues relate to system development and implementation, effectiveness, program management and oversight, and privacy and redress. We are also conducting our ongoing review in response to requests from the United States Senate: the Committee on Commerce, Science, and Transportation, and its Subcommittee on Aviation; Committee on Appropriations, Subcommittee on Homeland Security; Committee on Homeland Security and Governmental Affairs; Committee on Judiciary; also the House of Representatives: Committee on Transportation and Infrastructure, Committee on Homeland Security; and the Chairman of the Committee on Government Reform.

[2] GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*, GAO–05–356 (Washington, D.C.: March 2005).

[3] This statement does not provide information on the area of congressional interest related to modifications with respect to intrastate travel to accommodate states with unique air transportation needs because data were not yet available to us on the effect of these modifications on air carriers.

[4] TSC was established in accordance with Homeland Security Presidential Directive-6 to consolidate the government's approach to terrorism screening, including the use of terrorist information for screening purposes. TSC is an interagency effort involving DHS, Department of Justice, Department of State, and intelligence community representatives and is administered by the Federal Bureau of Investigation.

[5] CAPPS rules are characteristics that are used to select passengers who require additional security scrutiny. CAPPS rules are Sensitive Security Information.

[6] Aviation and Transportation Security Act, Pub. L. 107–71, § 136, 115 Stat. 597, 637 (2001).

[7] TSA plans to use this centralized vetting capability to identify terrorist threats in support of various DHS and TSA programs. In addition to Secure Flight, TSA plans to use the platform to ensure that persons working at sensitive locations; serving in trusted positions with respect to the transportation infrastructure; or traveling as cockpit and cabin crew into, within, and out of the United States are properly screened depending on their activity within the transportation system. In addition to supporting the Secure Flight and Crew Vetting programs, TSA expects to leverage the platform with other applications such as TSA screeners and screener applicants, commercial truck drivers with hazardous materials endorsements, aviation workers with access to secure areas of the airports, alien flight school candidates, and applicants for TSA's domestic Registered Traveler program.

[8] The Intelligence Reform and Terrorism Prevention Act of 2004 requires that TSA begin to assume responsibility for the passenger prescreening function within 180 days after the completion of testing. Pub. L. 108–458 § 4012, 118 Stat. 3638, 3714–19 (codified as amended at 49 U.S.C. § 44903(j)(2)).

[9] This description of the Secure Flight system, as well as the graphic illustrating the system in figure1, is based on TSA's draft June 9, 2005, concept of operations, a document that gives a high-level overview of the Secure Flight system.

[10] TSA also plans to utilize a cleared list as part of the watch list matching process; the cleared list is composed of individuals who are frequently misidentified as being on the TSDB and who have applied, and been approved, to be on the list.

[11] These measures may include additional screening or other law enforcement actions.

[12] Some selectees will receive a boarding pass from air carriers, but be required to undergo secondary screening prior to boarding the aircraft, while other selectees will first be met by law enforcement personnel, who will determine if the individual should receive a boarding pass. In addition, air carriers, through their application of the CAPPS rules, may also designate a passenger as a selectee.

[13] Examples of higher-order sources include legislation, which may dictate certain requirements, and other system documentation, such as the operational concept. When requirements are managed well, traceability can be established from the source requirements to lower-level requirements and from the lower level back to their source. Such bidirectional traceability helps determine that all source requirements have been addressed completely and that all lower-level requirements can be verified as derived from a valid source.

[14] Key requirements documentation we reviewed included the Transportation Vetting Platform/Secure Flight System Requirements Specification (May 13, 2005), the Secure Flight System Security Plan (July 15, 2005), the Transportation Vetting Platform System Security Plan (July 15, 2005), Transportation Vetting Platform and Secure Flight Security Risk Assessment (July 15, 2005), and documentation called for under Federal Information Processing Standard (FIPS) 199 (August 23, 2005).

[15] The NIST requirements provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the Federal Governments. The guidelines apply to all components of an information system that processes, stores, or transmits Federal information.

[16] An authorization to operate is issued for the information system, if, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, agency assets, or individuals is acceptable.

[17] OMB, Circular No. A–11, Part 7, Sec. 300. *Planning, Budgeting, Acquisition, and Management of Capital Assets.*

[18] The DHS Investment Review Board also reviewed the CAPPS II program in October 2003 and authorized the program to proceed with the system's development.

[19] The Committee was established under the authority of the Homeland Security Act, Pub. L. 107–296, in accordance with the provisions of the Federal Advisory Committee Act (5 U.S.C. App.2). At the first meeting of the Committee, in April 2005, Secure Flight was recommended as a program for examination for numerous reasons, including the number of citizens affected by the program, weaknesses in the program's redress system identified by us in our March 2005 report, and the program's potential use as a model for other related DHS efforts.

[20] The Aviation Security Advisory Committee, now within DHS, was formed in 1989 to provide advice on a variety of aviation security issues.

[21] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, August 2005. Congress requested that the DOJ–OIG evaluate TSC's plans to support Secure Flight to report these findings to the House and Senate Appropriations Committees.

[22] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center*, June 2005.

[23] The current draft of the DTPG also includes several appendices that provide additional, detailed program information to airlines, including an Interface Control Document containing detailed technical information such as message content and screen layout, a high-level technical plan for implementing various components of Secure Flight, detailed programming specifications for message timing and instructions for various passenger vetting scenarios, a recommendation that the airline industry develop an industry standard method for communicating Full Name (FN) and Date of Birth (DOB), and the system operational test plans.

[24] Stress testing refers to measuring a system's performance and availability in times of particularly heavy (i.e., peak) load.

[25] According to the DOJ–OIG, when Secure Flight becomes operational, TSC anticipates a significantly greater operational workload as a result of the program and an increased need for staff, space, and funding.

[26] Correspondence to the Honorable Michael Chertoff, Secretary, Department of Homeland Security, October 27, 2005.

[27] CBP and TSA officials stated they will use this same network to transmit data for their respective international and domestic prescreening efforts. Different addresses on the passenger information will ensure that TSA and CBP data are routed to the appropriate handling agencies for screening.

[28] For international prescreening, name-matching is conducted using data elements from a passport, whereas passports are not required for domestic flights.

[29] We currently have an on-going review of CBP's international prescreening process, including assessing the current process for conducting international passenger prescreening and reviewing the benefits and challenges of implementing additional or enhanced international prescreening strategies.

[30] Whereas stress testing is used to determine the maximum capacity of the system, operational testing is used to ensure that the system operates as intended, including the people and the information technology systems operating together in their expected environments.

[31] The name matching process depends on the level of false positive and false negative matches deemed acceptable. False negatives are passengers incorrectly not matched to a watch list.

[32] The score is based, in part, on how much weight is given to, say, name or date of birth relative to each other.

[33] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center*, June 2005. According to the DOJ Office of the Inspector General's report, some errors in the TSDB might be corrected by a manual review conducted by intelligence analysts and a redress process.

[34] We have an ongoing review of the reasons misidentifications occur using TSDB data, and the efforts by the TSC and other agencies to reduce these errors.

[35] Department of Justice Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, August 2005.

[36] Falsifying identifying information involves passengers attempting to hide their true identities by submitting fictitious identifying information, such as false addresses, when purchasing tickets. Identity theft would involve a passenger "stealing" another person's identifying information, such as name and date of birth, and then using that identifying information to create fraudulent documents associated with the identity (such as a driver's license containing the stolen identifiers with the thief's picture). This is sometimes referred to as identity fraud.

[37] The Department of Homeland Security Appropriations Act, 2006, Pub. L. 109–90, § 518 (e), 119 Stat. 2064, 2085 (2005).

[38] This prohibition on the use of appropriated funds does not apply to passenger name record data obtained from air carriers.

[39] GAO, *Aviation Security: Challenges in Using Biometric Technologies*, GAO–04–785T (Washington, D.C.: May 19, 2004).

[40] Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a).

[41] Also, in its mandate regarding Secure Flight, Congress asked that GAO review whether there are any specific privacy concerns with the technological architecture of the Secure Flight system.

[42] The Privacy Act requires that an agency publish a system of records notice in the *Federal Register* upon establishment or revision of the existence and character of any system of records. See § 552a(e)(4).

[43] The E-Government Act of 2002 requires agencies to conduct a privacy impact assessment before developing systems that collect, maintain, or disseminate information in an identifiable form. Pub. L. 107–347, 116 Stat. 2899.

[44] GAO, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO–05–864R (Washington, D.C.: July 22, 2005).

[45] See Pub. L. Nos. 108–334, § 522(a)(1); and 109–90, § 518(a).

[46] TSA's Office of Transportation Security Redress manages redress for the current watch list matching process conducted by the air carriers. Currently OTSR is developing an agency-wide policy for redress and has interviewed TSA Officials as part of this effort, but found that Secure Flight requirements were not sufficiently defined for use in drafting the new policy. TSA officials stated that they are continuing to discuss the Secure Flight redress process with OSTR.

[47] See Pub. L. 108–458, § 4012(a) (codified at 49 U.S.C. § 44903(j)(2)(C), (G)).

[48] This requirement generally addresses principles from both the Privacy Act—that individuals be able to access and correct their personal information—and the Fair Information Practice of individual participation—that individuals be able to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of such requests. However, Secure Flight's redress system will be challenging for two significant reasons. First, much of the information underlying decisions to add individuals to the TSDB is likely to be classified, and as such will not be accessible to passengers. Second, TSA does not control the content of the TSDB that it intends to use as the primary input in making screening decisions.

The CHAIRMAN. Thank you very much.

Mr. Hawley, since September 11th the Congress mandated multiple layers of security benefits to secure commercial aviation, including explosive devices—the explosive-device systems for baggage and hand screening procedures for passengers, expansion of the prohibited-items list, and hardened cockpit doors. New technologies, such as full-body imaging and explosive detectors for passengers, are also being deployed at airports by your agency to be used as secondary screening tools. With all of that, what really is the necessity for the Secure Flight Program?

Mr. HAWLEY. The Secure Flight Program is, I believe, an essential layer to that, which is to take known terrorists, who could be threats to the aircraft, and not let them get near the aircraft. And it's the requirement of the Intelligence Reform bill and the recommendation of the 9/11 Commission. So, it is a system that is essential and has continued to improve. And I'd like to just stress that every known terrorist, known to the U.S. Government, is, today, denied boarding. In the real world of today, that is in place. And it will become better when Secure Flight is implemented, but we're not waiting on Secure Flight for that.

The CHAIRMAN. How much has your agency spent to launch this and finish the Secure Flight Program? And what about the predecessor program, CAPPS II? I think we're interested in what we can do to assist, but it does seem that that program's taken a lot of money, and there are others coming.

Mr. HAWLEY. Yes, sir. $144 million, I believe, is the money for Secure Flight. CAPPS II was a program that started off as a program to evaluate the security risk of the passenger. It was discontinued toward the end of 2004, and Secure Flight went forward at that point, just for the terror watch-list matching. I think you put your finger on one of the key problems here is that the architecture

of CAPPS II, which was the original system, was used as the base for building Secure Flight on out, and the review that we're doing now says, "Let's just rebaseline it and say we're going to do just the terror watch-list matching, and go from there."

The CHAIRMAN. I don't want to embarrass anybody, and I don't want to get in any trouble at home, but we have people like Ted Kennedy being stopped, my wife, Catherine Stevens, being questioned whether she's "Cat Stevens."

[Laughter.]

The CHAIRMAN. How do people get off these lists? How do they prevent from being approached in a redundant way once that's been established?

Mr. HAWLEY. There is a process called the Redress Office, where we have a phone number and website, that the people who have familiar names—or names that are close to those of terrorists. They provide additional data. We give them a special number that then goes into their passenger record, and that list is actually kept, so that if they show up, they are removed from that confusion. And when it comes into Secure Flight, into the government, the system will run a little bit better, because it'll be totally automated, whereas, now it's part of the airline process.

The CHAIRMAN. OK.

I'm going to shift to you, Ms. Berrick. I think that the Congress mandated the GAO study ten elements of this program, Secure Flight, and it seems to me that TSA has an impossible task to move forward because of the criticism it's received from your agency on complying with those ten points. Aren't you really holding up moving on to further actions by the detail of the criticism you've given for so long on Secure Flight?

Ms. BERRICK. Thank you, Mr. Chairman.

We are mandated to look at those ten issues, and we have been working with TSA to be clear on the criteria that we're using to assess the program. But I think the real reason for the program delays hasn't been the review; it's been, first of all, I think, a lack of key policy decisions made by DHS and TSA regarding some critical aspects of the program that haven't yet been decided. The big decision that hasn't yet been made is what data TSA and DHS will require air carriers to provide. The air carriers are waiting for a rule to be issued. That rule has been pending for quite some time and hasn't been issued.

I think another reason for the delay is DHS's oversight over Secure Flight. DHS has a mechanism in place called the Investment Review Board, where they look periodically at major IT investments at every major milestone, and at any time they feel the program needs to be reviewed, to make sure it's progressing. DHS hasn't reviewed Secure Flight in over a year through that Investment Review Board process.

And in addition to the development process of Secure Flight, the requirements haven't been fully defined. TSA isn't following their own established development process of major IT systems.

The CHAIRMAN. Well, how can they finish it if you constantly are asking them questions about what they haven't done? I'd like you both to give us a timeframe. Mr. Hawley, how much time and how much money have you spent on Secure Flight? And you tell us how

much money—how much time you've spent. But I'm interested in how many people you've got holding up the total number of people he's got. OK? Just for the record. *

The CHAIRMAN. Senator Inouye?

Senator INOUYE. We've been concerned about privacy. I'm certain you realize that. Yesterday, we had a hearing on cell-phone privacy. You've spent some time on security and privacy. How do you expect to approach this privacy problem?

Mr. HAWLEY. Senator, I think the "privacy problem," will not go away unless the system is designed from the bottom up, with every process done from the start with privacy in mind, that is the way that a system will be built that can go forward and give people in the public confidence that there's not going to be a privacy problem. And that is what we're doing in what I said today, recertifying the program will, in fact, do what I just suggested. And I believe that is the only way to do it. And, as we have known, we have tried very hard over 4 years to be perfect on privacy, and that is very hard, unless the system is built specifically with that in mind.

Senator INOUYE. Is it true that your agency is considering using private vendors to access information, personal information, instead of the Government?

Mr. HAWLEY. For Secure Flight, no. For Registered Traveler, which would be a voluntary program, private-sector program, there is a possibility that they would use private-sector operations for that.

Senator INOUYE. The GAO has suggested that they have some difficulty determining how much has been spent. Do you have any idea?

Mr. HAWLEY. Yes, I think that we've got a good handle on how much is being spent. So, 144 million, I think, is the number. The issue that I hear from the GAO is, "Your management controls, which go to being able to see whether you're on target or off target, are not as specific as they need to be." And I think that's a fair criticism.

Senator INOUYE. Do you agree?

Ms. BERRICK. We've been unable to identify specifically how much has been spent on Secure Flight and its predecessor. We're estimating about 132 million, which is pretty consistent. One of the problems we've identified, though, as they're moving forward, the need for TSA to develop life-cycle cost estimates, and how much they think this program will cost in the out years. And that's one of the areas that we think that TSA needs to focus on.

Senator INOUYE. Mr. Hawley, I've been told that you're considering using private screeners to run your Registered Traveler Program. Is that authorized under the law?

Mr. HAWLEY. Yes. It is simply the same program that exists for every other aspect of TSA screening, that if the airport requests some combination of public and private, or all private, or all public, it's my understanding that is allowed under the law. And so, our attitude is, we exist only in airports, as far as aviation is concerned, and we take very seriously the request of the local airport.

---

*The information referred to is printed in the Appendix.

Senator INOUYE. What about fraudulent or stolen identities? Are you being able to cope with that?

Mr. HAWLEY. That is one of the major problems, I think, in security, is why you spend a lot of time understanding who the known terrorist is when that person doesn't use their name. That is a challenge. And it is something that has to require the different layers of detection, which include—that was where I mentioned CAPPS and the behavior aspect. And it's something that we're working very hard. And I think, as you know, we've done some pilots in the last couple of months that would add further layers directed at the unknown terrorist.

Senator INOUYE. Ms. Berrick, my final question, do you think that the Secure Flight concept is sound and worth the effort?

Ms. BERRICK. I think the program has the potential to provide some significant security benefits. The problem is, it hasn't yet been proven whether or not it will do so. Some of these policy decisions I mentioned that haven't yet been made have the ability to significantly influence how effective this program is, including how many additional people will be selected for screening. So, until these decisions are made and TSA follows this process that we've talked about to identify what capabilities they're going to deliver, it's difficult to determine what impact the system will have on aviation security. But I think the potential is there that it could strengthen aviation security.

Senator INOUYE. So, it's worthwhile proceeding?

Ms. BERRICK. I think so. I think it's important that TSA stop and rebaseline their program, as they're doing, define their requirements, and that DHS hold TSA accountable for making progress on meeting those requirements, within acceptable levels of cost.

Senator INOUYE. Thank you very much.

Ms. BERRICK. Thank you.

Senator INOUYE. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Nelson?

Senator BEN NELSON. Thank you, Mr. Chairman.

Mr. Hawley, I've had constituents from Nebraska whose names were put on a terror watch list. We've eventually gotten them removed by going through the process that you've outlined. Can you, without revealing anything that shouldn't be revealed, give us some idea about how that could happen?

Mr. HAWLEY. Sure.

Senator BEN NELSON. It wasn't like "Cat Stevens," or it wasn't something that was specific. These were fairly generic names. For the life of me, I could not understand how their names got on there. And we did have, initially, some significant difficulties in getting them removed—much, much more so than I would have expected.

Mr. HAWLEY. That part of the program, the so-called "redress," has improved as we've gone along, and just like the rest of the program, needs further improvement. But the way it works——

Senator BEN NELSON. Well, I can understand that. But how—I mean, I—I'm glad it's being improved. But how could it have been so flawed at the beginning? That's my question.

Mr. HAWLEY. It's that a terrorist is identified, and that individual has a name and other identifying characteristics. And, un-

fortunately, there are a lot of people who have similar names; and, in many cases, the same name; and, in some cases, the same "other identifying information." So, what's happened is, there is a terrorist that's using your name, and, once we figure out that the Nebraska person—what their identity is, and then we get their identifying information, we put that in the system, and then they are not confused as the terrorist, at that point. But it is possible that when somebody's added to the terror watch list, that everybody that flies with that identical name is going to have the first-time problem.

Senator BEN NELSON. OK. But it is being corrected. Do you have any indication, in terms of numbers, of how many people have had to go through that redress process?

Mr. HAWLEY. I know we have it. I don't have it, off the top of my head. But we can——

Senator BEN NELSON. Could you give me that?

Mr. HAWLEY. Certainly.

Senator BEN NELSON. Because it seems like it might be disproportionate. I didn't know there were a lot of people with the last name "Moore" that would have necessarily been on that list, so maybe you need to know more about that.

And then I did mention the two-tiered system, which I can understand for air fares, but I don't understand for security purposes.

Mr. HAWLEY. Yes, sir. The rules are, you enter TSA's checkpoint at the point that you present yourself to the screener, essentially, and that the airline has the responsibility of line management. So, it is at the discretion of——

Senator BEN NELSON. The airline or the airport?

Mr. HAWLEY. The airline, I believe.

Senator BEN NELSON. What if there are multiple airlines using——

Mr. HAWLEY. Yes. Well——

Senator BEN NELSON.—the same security?

Mr. HAWLEY. There is an agreement that's worked out, of actually fairly longstanding practice, of how to work that out.

Senator BEN NELSON. Well, I——

Mr. HAWLEY. In other words, it's not a TSA decision that says there should be X number of lines.

Senator BEN NELSON. OK. You think that's OK? We pay—we all pay the two-fifty for each segment of the flight, but we get different treatment at the airport prior to security.

Mr. HAWLEY. Well, when you show up to a TSA employee, we treat people the same, unless there is a security reason not to.

Senator BEN NELSON. All right.

With respect to the Registered Traveler program, you said that it's going to be paid for by the people who voluntarily submit themselves to that program. What about recovering developmental costs?

Mr. HAWLEY. Our plan is to cover the costs of the total program by those who use it. And I have just been provided the answer to your question about how many, and the answer is 30,000 total, or about 1500 a week.

Senator BEN NELSON. That end up on that——

Mr. HAWLEY. Redress list.

Senator BEN NELSON.—redress list.

What about—do we know what the costs have been for development of the Registered Traveler program? And do we have an indication of how many people are going to use it, so that we get a quantifier of what it's going to cost per person, so that there is a recovery of the costs?

Mr. HAWLEY. It's a market-based program, and we've worked very hard to get the lines for everybody down to a very manageable length of time. And that effort continues to be successful, which may lessen the market for a Registered Traveler Program. That's why we left it to the private sector, that says if there is, in fact, a market, they will make themselves known, they'll figure it out. But, from the TSA point of view, we did not feel it was essential for us to invest taxpayer money to go figure out the answer to that question.

Senator BEN NELSON. Well, I would agree, if—except for the fact that there's also a risk analysis going along with it, and if you have the Registered Traveler program in place, you would theoretically, and hope in actual practice, be the case that you would have less risk associated with those registered travelers; therefore, you could spend less time on them, more time where the risk could be greater, because the unknown and the uncertainty factors are there. So, they're really—I mean, I don't mind going to the outside to pay for it, but I think there is a cost savings associated with your agency not having to have personnel spend time on registered travelers, not because they've got priority treatment, but because they represent less of a risk.

Mr. HAWLEY. Yes, sir, we agree with that logic.

Senator BEN NELSON. So, I guess I'm not objecting to your going to the outside; I don't see the logic for going to the outside.

Mr. HAWLEY. It's that we have other priorities that are more important; and sometimes in making priorities the Secure Flight is a bigger priority for us than Registered Traveler. And these other layers of security, we feel, are critical. And it's a question of bandwidth, it's a question of money.

Senator BEN NELSON. In terms of any kind of a cost-benefit analysis for Secure Flight or Registered Traveler, do you feel that you've been able to—you said that trying to get the costs are hard to determine, but have you developed a cost-benefit analysis that might help us shed some—might shed some light on whether we're improving security or we're just keeping people busier going through the airports?

Ms. BERRICK. Yes, Senator. One of the things we looked at for Secure Flight—and we didn't look at Registered Traveler—but with Secure Flight, we looked at: To what extent did TSA develop, first of all, a cost-benefit analysis and then define requirements and then pursue development of this program? We found that TSA didn't develop a cost-benefit analysis for Secure Flight, specifically, so that there was nothing for us to review.

I wanted to make one comment about GAO's review of Secure Flight. The legislation requires that after TSA certifies that they have met these ten issues, then GAO has to assess their certification. So, the really—the next point in this process is TSA certifying that they've satisfied all these issues related to privacy and development. And it's not pending a GAO review; they can move

forward and do that at any time. But we'll continue to look at their development and privacy as they move forward with the program.

Senator BEN NELSON. Thank you.

And thank you, Mr. Chairman.

The CHAIRMAN. Yes, sir.

Senator Burns?

STATEMENT OF HON. CONRAD BURNS,
U.S. SENATOR FROM MONTANA

Senator BURNS. I keep looking at TSA, screening and airport security. I wish we'd have stayed with my amendment on the floor and put airport security in the Department of Justice and let the marshals do it. Then we wouldn't be meeting here today. We'd probably have these programs already in place. But we lost that fight, and now we've got to deal with this.

I had the same problem with a couple of my constituents in Montana that Senator Nelson had. And it took us a year and a half on one, and I've still got one in there. And the only place that this guy is dangerous is on a golf course.

[Laughter.]

Senator BURNS. And I just fail to see, whenever you've got affidavits and everything else identifying this guy, why—and if he's traveling with someone, Mr. Hawley—they take his wife or the couple they may be traveling with and question them? They make a lot of trips back and forth between Montana and Arizona, and every time, they go to the room, and everybody that's traveling with him goes too. So, I just wish that somebody down there would respond to those things. I understand the need for security. We're not complaining about that. And so does he. But he has to put another 30 minutes on his airport time, knowing that he's going to go to the little room. And that's very unhandy.

Let me just ask a couple of questions on this particular program. Say that I have a card for this program. I've paid for it, I've complied with all the information. Does your department keep a database to keep track of my travel, or is that information cleared from the record at a certain point? I mean, how long do you keep the records of my travel and travel movements, or do you keep a database on it?

Mr. HAWLEY. Well, we don't get it for Secure Flight. It's a bouncing mechanism that says, Is this person on the watch list, or not—yes or no? And that's the end of it.

Senator BURNS. That doesn't record the amount of times that I have walked through security to board an airplane?

Mr. HAWLEY. No.

Senator BURNS. It's not.

Mr. HAWLEY. Not to my knowledge. Yes, 72 hours after the trip, we delete the record.

Senator BURNS. You clean the——

Mr. HAWLEY. Delete it.

Senator BURNS. You clean the records.

Mr. HAWLEY. Yes.

Senator BURNS. Now, if a person is rejected, what is the process or the protocol for explaining why they were rejected? Is there a protocol? Do you give them the reasons why they were rejected?

Mr. HAWLEY. In most cases, no. Now, if the person is a mistake, then clearly yes. That's a mistake, you shouldn't be on the list, there's a number you call, there's a way you get yourself off the list. But if someone is on the list and is a terrorist, we do not feel the obligation to share with them everything that the Government knows.

Senator BURNS. OK. Now, I walked through a new machine at National the other day. They call it "the puffer," or something.

Mr. HAWLEY. Yes, sir.

Senator BURNS. Tell me the difference between that particular piece of equipment and the ones we've been using in the last year or so.

Mr. HAWLEY. The puffer technology dislodges explosive particles that permeate you or your clothing or your belongings. And so, the puff of air dislodges some of that chemistry, it's brought up into the top of the machine, where it goes through an analysis that is essentially the same one that happens when they do the swab of your material. It's the same technology, to compare that with the known explosive. So, that's what the technology is. It's a different way. Instead of rubbing the surface, it dislodges some of the small particles.

Senator BURNS. I just thought of something. Are they going to ask you to survey on what kind of aftershave we're using, or anything like that?

Mr. HAWLEY. As long as it's not explosive, you'll be fine.

Senator BURNS. OK, just explosives. That's a good thing.

[Laughter.]

Senator BURNS. That's a good thing.

And that's all I have, Mr. Chairman. I just wanted to ask about those particular items of concern for some of my constituents that travel quite a lot. And I find more people are willing to join the Registered Traveler program, just because they like to go get on the airplane. And so, that's it. But thank you very much.

Ms. BERRICK. Senator, if I could add, quickly, the redress process that Mr. Hawley just explained was for the current prescreening process that the air carriers maintain. The redress process for Secure Flight hasn't yet been fully defined, and that could also impact how long data is kept after the process, so that TSA could go back and make any corrections.

Senator BURNS. Yes, we have a tendency to run both of the programs together, and I'm sorry about that. I didn't make that clear.

Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you very much.

Mr. Hawley, I wanted to arrange a classified briefing with you—I want to arrange a classified briefing with you on how this intersects with our information systems that will lead to intelligence-sharing. So, if we keep that in mind——

Mr. HAWLEY. Yes, sir.

The CHAIRMAN. I don't know what your timeframe is, but I do want the Committee to have a further briefing on the interlocking between this system and the intelligence systems that are further designed to assure the traveling public has the security it needs.

We thank you both for being with us today. Thank you very much.

Ms. BERRICK. Thank you, Mr. Chairman.

The CHAIRMAN. Did you have any further questions, Senator?

Our next panel is Jim May, the Chief Executive Officer of the Air Transportation Association; Charles Barclay, President of the American Association of Airport Executives; Tim Sparapani, Legislative Counsel for Privacy Rights at American Civil Liberties Union; and Bill Connors, the Executive Director, Chief Executive Officer of the National Business Travel Association.

Ms. Snowe is here, and I failed to recognize her to put her statement in the record if she wishes. I know she had another commitment at Finance.

We're pleased to have you with us this morning, gentlemen. As I indicated before, your statements automatically go in the record as though read, and we'll be pleased with your summaries.

Mr. May, we'll call on you first.

STATEMENT OF JAMES C. MAY, PRESIDENT AND CEO, AIR TRANSPORT ASSOCIATION OF AMERICA, INC.

Mr. MAY. Thank you, Mr. Chairman. In the interest of time, I'd like to summarize even my oral statement and make a couple of fundamental observations.

First, I'd like to thank the Committee for again taking a principled stand that aviation security is a function of national security, and should be paid for as such. Regrettably, not everyone agrees with that. And as a result, we have more proposals from the Administration, trying to increase the security fees that we pay today.

I think it's important to put that in context as we begin this debate on Registered Traveler and Secure Flight, because when TSA was started up, it had a budget of roughly $4 billion; today it has roughly the same budget. We started paying fees, back in 2002 to TSA, that aggregated somewhere a little over $1.2 billion, just strictly to TSA. We have three other fees that we pay to other elements of the Department of Homeland Security. I think we're the only transportation mode that pays those. And those fees have now grown, in aggregate to DHS, to about $4 billion a year from that initial beginning of $1.25 billion or $2.6 billion. And we now have proposals for an additional billion-four on top of what we're already paying.

So, we not only care about the business of security from the perspective of trying to have our passengers, your constituents, move through airports as quickly and efficiently as possible, but we care from the perspective of the amount of money that we're being charged, and our passengers are being charged, every single year by the Department of Homeland Security and TSA. And I hope that provides some perspective.

Now, when it comes to the Registered Traveler program, you know, there's an old line in song about "being country before country was cool." ATA was one of the original supporters of a registered-traveler program, but let me ask you to think back to that time. That time was when we had not only people going through security, but, once you got to the gate, you had to go through the gauntlet one more time. And the likelihood is, if you were the third person to go through, everybody knew you were going to get pulled

aside, and you'd get searched and wanded, and you'd have to dump all your materials out onto a folding table and so forth. And so, we, at that point, said, look, let's try and expedite this process a little bit, and maybe we can have a registered-traveler program.

I hate to think about how much money has been wasted on the RT and the Secure Flight programs since that time, but the good news is that the process has improved dramatically. We got rid of the gate check, we're doing other measured improvements to security. People are acustomed to going through the process. And instead of having those 2-hour waits, we now have, believe it or not, about a 10-minute wait, on average, throughout the system. So, the need for that Registered Traveler program that we first envisioned, I don't think is there.

What we really need to do today is get the TSA to focus on improving the process for all passengers, not a select few passengers. We need to get the better technology, the puffer technology that Senator Burns, I think, talked about. We need to make sure that we move through crews and pilots in a quicker way, because they are already certified to go through the process. We need to have more technology, as I said, and we need to get the TSA to start putting their part-time workers on during peak periods. I think if those changes are made, we're going to see the process for everybody improve dramatically.

Now, as to the RT program itself—or, I'm sorry, the Secure Flight program itself, I'd like to point out to the Committee that it's not just the Secure Flight program. We, as airlines, have had to deal with CAPPS, with CAPPS II, with Secure Flight, with Registered Traveler, with APIS, with APIS Plus 60, APIS AQQ, the CBP's PNR access program, and, most recently, we're being asked to comply with a bunch of requirements on data collection by CDC as it relates to avian flu. So, we are facing seven different government programs, all of which are intended and directed at passenger prescreening. There are some 34 different data elements that we're being asked for. And there are at least 20 countries around the world that have similar kinds of programs. In my written testimony, I've suggested a series of things that can be done to simplify that process, but we are being inundated with data requests.

So, our real request to this Committee is, please force TSA, force DHS, force CBP, force all of these different agencies to come up with a single simple template that can be used against the watch list, that can be used against other programs, and go forward with that, put your energies there, along with technology increases, so that we move everybody through the process more quickly than we are today, not just a special few who are willing to pay a great deal of money to become registered travelers for what I, personally, believe are going to be very limited benefits.

Thanks for your time. I'm happy to answer any questions.

[The prepared statement of Mr. May follows:]

PREPARED STATEMENT OF JAMES C. MAY, PRESIDENT AND CEO, AIR TRANSPORT ASSOCIATION OF AMERICA, INC.

No consumer service industry is affected by security requirements like the U.S. airline industry. That central fact significantly shapes the economics of providing air transportation. Yet the airline does not control this situation because civil aviation security in the United States is a Federal responsibility. This is as it should be but

does not diminish the airline industry's very legitimate interest in seeing that security-related measures are effectively conceived and properly and economically implemented.

In the last several years, the Transportation Security Administration has clearly improved its screening of passengers and their baggage. Anyone who regularly travels by air has witnessed that improvement. And TSA has emphasized its commitment to using risk analysis to establish security priorities. These developments are encouraging and should be recognized.

Nevertheless, important elements of the government's aviation security programs are not nearly as cohesive or well founded as they could be. There is no justification for this. Aviation security is obviously dynamic but in these matters, to mix a metaphor, we should have gotten our sea legs by now. We need to do so quickly.

Today's hearing is thus exceptionally important and timely. It is an opportunity for us to focus attention not only on the Secure Flight Program and the Registered Traveler Program but, equally important, also on other existing and emerging aviation security programs that will impose substantial new information demands on passengers and airlines. The characteristic that is common to these programs is their dependence on passenger information. That is where the commonality ends. These programs are uncoordinated, which is inexplicable and should attract close attention. Intuitively, most of us would assume that considerations of efficiency would have produced far more commonality among Federal programs that are both security oriented and data dependent. The fact that this has not happened should prompt an examination of their *efficacy*—how well they achieve their stated aviation security objectives; their *efficiency*—how economically they accomplish those objectives and whether less costly alternatives exist; and their *protection of privacy*—how thoroughly they preserve passengers' expectations of privacy, and how adequately and transparently they delimit governmental agencies' use of personal information.

TSA's Secure Flight Program and its Registered Traveler Program illustrate the complexities of data-based security programs and, in the case of Registered Traveler, the need to return to first principles when evaluating them.

Secure Flight is intended to pre-screen airline passengers. As envisioned, an airline would submit to TSA certain passenger information whenever a reservation is made for a domestic flight. It would enable TSA to compare reservation information with the Federal Government's no-fly and selectee lists. TSA expects that this arrangement will enhance security, improve pre-screening efficiency and reduce the number of passengers subjected to secondary screening. Each of these outcomes would be very desirable.

Airlines and ATA have worked with TSA at several points in its development of Secure Flight. We have also worked with CBP and CDC on their passenger information needs. This experience has left two important impressions. First, coordination between government agencies and airlines is essential. Any program that involves government access to reservation information generates substantial data content, format and transmission issues. You cannot simply push a button to get passenger data that would be useful to TSA or any other Federal agency. Second, privacy issues are of the utmost significance in any government program to access passenger data. Privacy issues are an immutable part of the landscape.

The nature of Secure Flight is such that the airline industry's involvement with TSA about it, necessarily, has been limited. Nevertheless, we are hopeful that its benefits can be soon realized.

In contrast to our hopes about the Secure Flight Program, the Registered Traveler Program has turned into a shifting and dispiriting exercise. It compels you to ask, "Where's the beef?"

The airlines were early and ardent advocates of the registered traveler concept. Four years ago we urged the development of a government system that would speed the screening of those passengers who did not present security concerns and thereby facilitate the processing of the vast majority of travelers. Today's Registered Traveler Program promises no such benefits to our customers. Indeed, the Registered Traveler Program as currently constituted has become even less attractive because it has been morphed into an orphan program; TSA has largely lateraled it to the private sector. Finally, the systemwide improvement in passenger screening that TSA has accomplished in the last few years begs the question of why this sorry state of affairs should continue.

We are unaware of any evidence that Registered Traveler will produce the tangible and widely available benefits to passengers that we had envisioned in 2002; or that it will attract significant numbers of registrants; or that it will generate a pronounced improvement in overall security; or that vendor interoperability issues will be overcome; or that systemwide passenger wait times will diminish; or that passenger privacy issues have been confronted and satisfactorily resolved. We, how-

ever, do know that what was originally conceived as a straightforward governmental program to benefit the vast majority of passengers has been transformed into a commercial enterprise for what increasingly looks like the few.

Registered Traveler neither offers the benefits to passengers nor the breadth of use that justify its introduction as a permanent program. It should be eliminated.

As I observed at the beginning of my testimony, other existing and contemplated aviation security programs rely or will rely on government access to passenger information. Expanding passenger information requirements create substantial new demands on governmental agencies, airlines, and travelers. The problem is that government passenger information requirements thus far have only produced a mosaic. It remains to be seen if a coherent a picture will emerge.

This is a serious situation. Given the security threats confronting civil aviation, there is no reason to believe that the government's passenger information needs will abate. Passenger data will be required for the Secure Flight program and the Registered Traveler program. In addition, passenger information is currently required for CBP's Advance Passenger Information System and CBP's passenger reservation information access program. Moreover, foreign governments are imposing similar demands on airlines flying to their countries, including U.S. air carriers. This unmistakable international trend is most evident with the ever-increasing number of countries that require APIS information but also is reflected in the Canadian requirement for access to passenger reservation information for international flights bound for Canada, including flights from the United States. Finally, the Centers for Disease Control has proposed a rule that would require that airlines collect and store broad new categories of passenger contact information.

Information management is precisely where the government should be able to achieve a coherent policy. We appreciate the ongoing efforts of CBP and TSA to more closely align APIS and Secure Flight data requirements. However, the continued absence of a comprehensive, government-wide passenger information access policy is a matter of real concern to us. Nor is there any indication that any element of the Federal Government is inclined to assume the responsibility to develop and oversee such a comprehensive policy.

This needs to change quickly. The U.S. Government must produce a uniform passenger information collection policy that applies to all of its civil aviation security and facilitation programs. Our government should also lead an effort to create such a policy for worldwide application.

A workable government-wide passenger information policy should be predicated on four fundamental considerations.

The first consideration is the recognition that a uniform policy is indispensable to the efficient collection, retention and use of passenger information. Multiple, uncoordinated information demands do not advance aviation security. Instead, they create unneeded complexity, wasteful duplication, and unjustifiable costs to the government, customers and airlines.

The second consideration is that a uniform policy must be based on a single passenger information template that contains the only authorized categories of data that a Federal agency can require collection of or access to. Agencies should be prohibited from imposing unilateral data requirements that go beyond the template. A uniform policy means no ad hoc data requirements.

Similarly, uncoordinated methods of data transmission are unnecessarily complex and costly. This is not the forum to explore how best to resolve this issue. But I want to highlight the importance of working as best we can to develop a single "pipeline" to transmit passenger data to Federal agencies. Independent transmission channels to multiple Federal agencies mean duplicative work for both airlines and the government, and the unnecessary cost and drain on scarce resources that inevitably result from such inefficiency.

The third consideration is that the justification for every passenger information collection program should be evaluated under uniform criteria. The needs of individual agencies may vary but the conditions under which any agency is permitted to collect or access passenger information should not vary. Six basic criteria should be relied upon:

- **Demonstrate civil aviation security or facilitation need.** A clear, direct relationship between the security threat or facilitation need and the information sought should be demonstrated. Presumably, this will be tied to the agency's risk assessment. Data needs not associated with security or facilitation should not be part of any passenger information program.
- **Minimize data demand.** Data required should be the minimum necessary to fulfill an agency's needs. This will reduce impositions on passenger privacy and diminish airline compliance costs.

- **Use existing information sources.** To the extent feasible, agencies should rely on existing government passenger information programs to fulfill their data needs.
- **Avoid adverse effects on passenger processing.** Information collection requirements must avoid adversely affecting passenger processing, whether during the reservations process, airport check-in, security screening, or arrival in the United States from overseas.
- **Conduct thorough cost evaluation.** Passenger information collection, storage and transmission costs, as well as individual passenger compliance costs must be recognized and carefully evaluated. A cost-benefit analysis based on these factors should be undertaken for each information collection or access program.
- **Minimize false hits.** If passenger information is used to evaluate a passenger for security purposes, the program must contain measures that minimize false hits and enable the agency to evaluate its false hit experience.

The fourth consideration is that the privacy implications of any proposed passenger information requirement must be rigorously examined before the implementation of such a program. This is a matter of both accountability and legitimacy. It is a matter of accountability because the government should not demand personal information without performing such a careful analysis. It is a matter of legitimacy because the traveling program will not long support a government-imposed information program that it believes does not scrupulously protect an individual's privacy.

At the very least, this means that government programs must adhere to privacy principles that focus on information collection purpose, content, retention and onward transmission limitations. In addition, a prompt and effective redress mechanism must be available to those customers who believe that they have been adversely treated.

Foreign governments' data privacy principles must also be taken into account because U.S. airlines that operate overseas are subject to them. Compliance in other nations is often enforced through both civil and criminal penalties. No U.S. airline should be subject to the conflicting requirements of the U.S. Government and a foreign government. This concern is very concrete. U.S. airlines operating to Europe confronted that prospect several years ago when European governments expressed skepticism about the adequacy of CBP's protection and use of passenger reservation information that it accesses. That situation has been resolved for the time being. It, however, left us with the clear realization that the U.S. Government—and not the U.S. airline industry—has the responsibility for resolving conflicts between its information requirements and the data privacy regulations of other nations.

My experience over the last several years with security issues has convinced me of several things. First, coordination between the government and industry at the outset of the development of any aviation security program is critical and is plainly in the interest of the government, customers, and airlines. Second, we know how to measure the effectiveness of these programs; we should not be afraid to apply to them appropriate metrics—including risk and cost-benefit analyses. Third, we need to formulate, in very short order, a coherent government-wide policy about passenger information collection requirements. Fourth, resolution of privacy issues is crucial to the success of these programs and that resolution is the government's responsibility.

Aviation security needs will change over time but the considerations that I have described in my testimony should facilitate prompt and effective responses to them, no matter how they may evolve.

The CHAIRMAN. Thank you very much.

The President of the American Association of Airport Executives, Chip Barclay.

Chip?

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

Mr. BARCLAY. Thank you, Mr. Chairman, Mr. Co-Chairman, Members of the Committee. It's always a privilege to appear before the Commerce Committee.

I'd like to make three points in summarizing our testimony.

The first is that airports continue to believe that the key lesson of 9/11 is that dangerous people pose the greatest threat to our system. On 9/11, the powerful weapon used against us was the terrorists' knowledge and manipulation of our hijacking policies of that day. And, while those policies have changed, what hasn't is that deliberate, smart terrorists will seek to exploit any system that we have or put in place in the future. So, in addition to other security efforts, we need to develop better tools that look for dangerous people.

That job has two components. One is identifying the people that don't pose a threat to the system, which is the great majority. And the second is identifying those few that present either unknown or potentially dangerous factors. Secure Flight appropriately seeks to go after that second goal, while Registered Traveler, or RT, offers a voluntary effective path to go after the first.

Registered Traveler provides an option for individuals to volunteer information on themselves, permit TSA to determine they don't present a risk to the system, verify their identity each time they travel, and those individuals will pay for all the costs of that program.

The privacy issues about both these programs raised by TSA and others during the hearing need careful attention and transparency in their resolution. But it is equally important to recognize that the constitutional protection to the right of privacy is not a right to anonymity. Accurate, verifiable identification is a reasonable request of each airline passenger as a tool for maintaining a safe public-transportation system for all airline passengers.

My second point is to let the Committee know that a significant group of airports and technology companies, some 70 airports and 40 companies, have collaborated, through an organization called the Registered Traveler Interoperability Consortium, to come up with a secure, nationwide, and interoperable Registered Traveler program. The recommendations leave key security standards and the approval of individuals as qualified for Registered Traveler to TSA, but accomplishes much of the remaining work through local airports in whose terminals the programs must operate, and TSA-certified technology companies that can enable the highly accurate and consistent operating process required.

My third point is that industry, local government, and Federal Government can work effectively as partners in security credentialing programs. One program the Committee has heard little about, because it's effective, efficient, and has operated without controversy, is the aviation-worker Criminal History Record Check for employees with access to secure areas at commercial airports. Prior to 9/11, fewer than 10 percent of aviation workers were required to obtain the CHRC checks through a Federally operated process. Those checks averaged, at that time, almost 2 months to complete, even though the FBI computer check of fingerprints usually takes only minutes. The system was fraught with black holes, poor communication, and no reconciliation of the process for end users.

Post-9/11 reviews brought a new requirement to have these criminal history record checks for all workers with access to secure areas at airports, which was about a million in the year 2002, as

well as a new organization, the Transportation Security Clearinghouse, that's operated by AAAE. The background checks that it does there, it does in partnership with airports, airlines, and TSA. (Initially, that was with FAA).

Four years later, the average criminal history record check takes 4 hours, instead of 52 days. The price per transaction has been reduced from $31 to $29, while an identical check for HAZMAT truckers costs $100. And the TSA has processed just shy of 2 million background checks, making it the largest such clearinghouse outside the Department of Defense in the last 4 years.

The most important of those facts is the time savings, from months to hours, of these checks. It represents personnel cost savings in our industry of hundreds of millions of dollars annually. This successful credentialing program works in a 24/7 realtime industry. Because it's an effective partnership of DHS, TSA, airports, airlines, and the Clearinghouse, each with well-defined roles, it's a model, we believe, for other programs and industries. And I've got some further information on that I'd like to add to the record, if I could.

Finally, Mr. Chairman, while not on point for this hearing, I do not want this opportunity to pass without a brief mention of another program over which the Committee has jurisdiction, the Aviation Trust Fund.

The Administration's budget request of earlier this week is seriously flawed from the perspective of the Nation's airports. As this Committee knows, as the author of the Aviation Trust Fund, it was originally designed to collect taxes from passengers for capital developments of the system, not for operations. The recent budget request turns that fundamental priority of the Trust Fund on its head, requesting large-operations budget increases while slashing the capital-improvement programs almost $1 billion from the AIP program from the level authorized by this Committee. We think such cuts are unwise and shortsighted, and we hope that the Committee will agree and fight to fully fund the capital programs.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Barclay follows:]

PREPARED STATEMENT OF CHARLES BARCLAY, PRESIDENT, AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

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

Registered Traveler, Secure Flight Effectively Focus Limited Resources on Greatest Risk

Let me begin, Chairman Stevens and Co-Chairman Inouye, by thanking you for your continued focus on the operations and priorities of the TSA. The programs the Committee has selected to examine today in the area of passenger pre-screening hold enormous potential in improving the effectiveness and efficiency of security screening operations at airports across the country. With aviation traffic returning to record levels and with Federal resources becoming ever scarcer, it is imperative that we get the most out of every dollar we devote to security. Utilizing better tech-

nology—such as Registered Traveler and Secure Flight—to effectively manage risk results in better security and a more efficient use of Federal and industry investments.

In our view, one of the key components to improving passenger screening is shifting the focus from finding dangerous "things" to finding dangerous "people." The most important weapon that the 19 terrorists had on September 11 wasn't box cutters; it was knowledge—knowledge of our aviation system and existing security protocols, which they used to their advantage. We simply must do more to identify potential threats. Secure Flight offers opportunity in that regard, although we recognize that it must be pursued with careful consideration provided to a full range of individual privacy issues.

Additionally, we must quickly take advantage of the opportunity that exists through deployment of a Registered Traveler program to more effectively calibrate the resource allocation at airport screening checkpoints. With more than 700 million passengers traveling through the U.S. aviation system each year—a number that is anticipated to grow to more than one billion annually within the next decade—we simply must take a better approach to security screening. Relatively few passengers make up the overwhelming majority of all travel, and we should make every effort to provide a different screening protocol for this group of travelers. Doing so will help expedite the screening process for all travelers and allow screeners to focus more intensely on unknown and potential threats.

Our challenge with regard to passenger screening remains to find the proverbial needle in the haystack. Registered Traveler can help reduce the size of the haystack, and Secure Flight can help ensure that more resources are devoted to finding the needle. Both goals are important, and both programs deserve the continued support of Congress and the TSA.

Along those lines, we are extremely encouraged by the leadership that Department of Homeland Security Assistant Secretary Kip Hawley has provided since taking over the helm of TSA and believe that he deserves a great deal of credit for recognizing the promise of these programs and for working to expedite their implementation. On Registered Traveler, in particular, Administrator Hawley has moved the program past the "pilot" program phase and announced a timeline for making a nationwide, interoperable program a reality by this summer. It is our sincere hope and expectation that the announced timelines will be met, and we look forward to continuing our work with TSA and the Congress to ensure that is the case.

Public/Private Partnerships Have Proven Effective and Should Be Further Utilized

While the Federal Government obviously plays a leading role with regard to passenger pre-screening and other areas of aviation security, airports and the aviation industry can and should play an active role in partnering with the Federal Government to design and implement meaningful solutions to security challenges. The establishment of effective public/private partnerships has already proven extremely successful, for example, in building a system for processing fingerprint-based background checks and additional background screening for more than 1.9 million airport and airline employees through the Transportation Security Clearinghouse. We believe that the public/private model offers one possible solution in the areas under discussion today.

On the Registered Traveler front as I will discuss in more detail, the representatives of the airport community and its aviation partners have proposed a public/private model that will be both interoperable and innovative. Undoubtedly, the best path forward is one in which Federal resources and standards are combined with the knowledge, expertise and creativity of airports, airlines and aviation-oriented businesses.

Secure Flight Is Critical Tool in Identifying Dangerous People

While the majority of my comments today are focused on Registered Traveler, I would like to highlight the critical nature of the Secure Flight program and to urge the Committee's continued support. While there are critical privacy issues that must be addressed, it is indisputable that the more we know about individuals traveling through the aviation system, the more secure it will be. In today's high-threat world, we must all recognize that the Constitutional right to privacy that we enjoy as Americans does not provide a right to anonymity.

Knowledge is power and the more we know about potential threats before they have a chance to proceed to a security checkpoint or board a plane, the better off we all will be. Secure Flight adds yet another critical layer of security to the system and ensures that we don't rely solely on physical screening to identify those who

seek to do us harm. Once privacy protections are ensured, the Federal Government can and should move forward with Secure Flight as soon as possible.

Registered Traveler Program Will Improve Security and Efficiency at Airports

Before discussing some of the specific efforts of airports to partner with TSA in making Registered Traveler a reality, it is important to highlight again the value of a nationwide program and to remind the Committee of the strong endorsement the concept received from the 9/11 Commission and numerous others. In an era of risk management, limited Federal resources must be focused on known and unknown risks to the aviation system. Registered Traveler accomplishes that goal by helping TSA to better align screeners and resources with potential risks.

Given existing traffic levels and anticipated system growth over the next decade, we simply must take a smarter approach to passenger screening. Today's personnel-dependent screening system is already being pushed to the brink. One can only imagine what the situation will become as 300 million or more additional passengers are added to the system.

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

We have learned a great deal from the recently concluded Registered Traveler pilot programs that involved five airports partnering with a single air carrier at each airport. Although the original TSA pilot programs were popular with participants, they were not interoperable by design, which limited benefits to only one air carrier at each of the five original airports. Additionally, participants largely were subjected to the exact same security protocol—the removal of laptops, shoes, and coats were still required, for example—as non-participants, meaning that the only real benefit was being moved to a shorter screening line with limited secondary screening.

Moving forward, it is clear that in order to realize the true potential of Registered Traveler, the program must be *nationwide and interoperable*. Participants who sign up in Phoenix, in other words, must be recognized and accepted as they travel to other airports that have chosen to participate in the program, be it Denver, Atlanta, Washington or other airports throughout the aviation system. Additionally, security screening protocols should be adjusted for program participants in recognition of the extensive background vetting they have received. Passengers who are willing to provide substantial background information and undergo government security threat assessments should be accommodated with tangible screening benefits, such as non-divestiture of shoes, outer garments and laptops.

As TSA proceeds with implementation of the Registered Traveler program, it is also important to note several potential pitfalls that the Federal Government must work to avoid. First, Registered Traveler cannot be viewed within DHS and the Federal Government as simply a way to save money or to compensate for insufficient screening resources. At its core, Registered Traveler is a security-based program that will augment other screening efforts and better focus resources. It cannot be used as an excuse to shortchange other screening needs. To that end, we again call on TSA to issue and publish performance standards for security screening that apply to all screening locations.

Additionally, the Federal Government must ensure that all data collected in conjunction with Registered Traveler is fully secure. TSA needs robust safeguards to protect proprietary data it will collect through the program's implementation. Such assurances are critical to ensure participation by the traveling public. Potential Registered Traveler program participants have a right to expect that these issues will be addressed before implementation just as all individuals have a right to expect that privacy issues will be addressed before Secure Flight becomes operational.

Finally, all fees associated with program participation must be transparent, cost-based, and kept to a minimum. The cost component is critical if we expect this voluntary program to work as promised.

Airport Registered Traveler Interoperability Consortium (RTIC)

As I now turn to the Registered Traveler Interoperability Consortium (RTIC), I would note that ACI–NA is not a party to the RTIC process. As such, the following comments on the consortium reflect only those of AAAE and are specific to the 70 airports and 40 service providers that participated in the RTIC process.

Airports, in light of their public nature and responsibilities to the communities they serve, remain eager to partner with the TSA to improve the effectiveness and efficiency of the security screening process. In recognition of the promise that Registered Traveler in particular holds in achieving these goals, airport professionals have been working diligently to move forward operationally with the program. The RTIC represents one voluntary initiative focused on that goal.

The RTIC is a group of more than 70 airports and 40 service providers that have worked for the past six months to define and establish the mutual and common business practices and technical standards that will complement Federal standards and help push forward a national program. RTIC represents a significant attempt by a large group in the airport community to partner with TSA in making the promise of RT a reality as quickly as possible.

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

Current Airport Members of the RTIC Include the Following Arranged by Size (Enplanements) Based on Calendar Year 2004 Data

Hartsfield-Jackson Atlanta International Airport
Denver International Airport
Phoenix Sky Harbor International Airport
John F. Kennedy International Airport
Minneapolis-St. Paul International Airport
George Bush Intercontinental/Houston Airport
Detroit Metropolitan Wayne County Airport
Newark Liberty International Airport
Orlando International Airport
Miami International Airport
Seattle-Tacoma International Airport
Philadelphia International
Boston Logan International Airport
New York La Guardia
Washington Dulles International Airport
Baltimore-Washington International Airport
Fort Lauderdale/Hollywood International Airport
Ronald Reagan Washington National Airport
Pittsburgh International Airport
Lambert-St. Louis International Airport
Memphis International Airport
Nashville International Airport
William P. Hobby Airport
Austin-Bergstrom International Airport
Palm Beach International Airport
General Mitchell International Airport
Port Columbus International Airport
T.F. Green State Airport
Reno/Tahoe International Airport
Ted Stevens Anchorage International Airport
Manchester Airport
Tucson International Airport
Louisville International-Standiford Field
Albany International Airport
Lihue Airport
Gerald R. Ford International
Des Moines International Airport
McGhee Tyson Airport
Wichita Mid-Continent Airport
Palm Springs International Airport
Tallahassee Regional Airport
Huntsville International-Carl T. Jones Field
Lexington Blue Grass Airport
Atlantic City International Airport
Northwest Arkansas Regional Airport
Newport News/Williamsburg Int'l Airport
Santa Barbara Municipal Airport
Fort Wayne International Airport
Daytona Beach International Airport
Roanoke Regional/Woodrum Field
Bangor International
Yeager Airport
Wilmington International
Chattanooga Lovell Field
Kalamazoo/Battle Creek International Airport
Jackson Hole Airport
Cherry Capital Traverse City Airport
Monterey Peninsula Airport
Lafayette Regional Airport
Redmond Roberts Field Airport
Grand Forks International Airport
Waco Regional Airport
Redding Municipal Airport
Greater Rockford Airport
St. George Municipal Airport
Flagstaff Pulliam Airport
Barkley Regional Airport
Tupelo Regional Airport
Pullman/Moscow Regional Airport
Mid-Ohio Valley Regional
Shenandoah Valley Regional Airport
Dickinson-Theodore Roosevelt Regional Airport

For the past six months, members of the RTIC have been working diligently to establish and agree on common core principles that will enable technical interoperability across a broad and varied airport network. In comments filed with TSA in late January in response to the Agency's Request for Information on the Registered

Traveler program, RTIC and its Service Provider Council provided a detailed series of agreed upon financial standards, technical interoperability standards and common business processes for the program.

These recommendations provide a consensus framework for rapid, secure, and seamless deployment of a Registered Traveler program at the Nation's airports that will result in enhanced security and quicker security processing. It is our hope that these consensus recommendations will be adopted by TSA as the agency moves forward with program implementation.

While we would be happy to offer the Committee details on the RTIC filing with TSA, we wanted to simply summarize those efforts here. With regard to common business processes, the RTIC has identified each of the key players in a national, interoperable RT program—enrollment service providers, verification service providers, the Registered Traveler Management System, TSA, applicant and participant—and detailed the potential roles and responsibilities of each. On technical operability, the RTIC has made specific technical recommendations on system messaging, ensuring a chain of trust, optimizing the use of biometrics, leveraging appropriate token technologies, ensuring system security, protecting privacy, and ensuring cross-provider interoperability. In the area of financial standards, RTIC has proposed a simplistic and straight-forward approach to enabling the maximum flexibility and competition for solutions for both enrollment and verification service providers.

The RTIC is committed to working closely with TSA to meet the timeline established by the agency and its pledge to: use a public-private partnership model, build off of existing security networks through utilization of the Transportation Security Clearinghouse, establish a sustainable, biometrically enabled and interoperable system, and establish a program where travelers will receive screening benefits through in-depth background checks.

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

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

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

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

ADDITIONAL INFORMATION SUBMITTED BY CHARLES BARCLAY

Airport Magazine, May/June 2005 Issue

INSIDE TSC: SAVING MONEY, SAVING TIME

Compiled From AAAE Staff Reports

A dramatic reduction in fingerprint processing time from 52 days to four hours that saves the aviation community hundreds of millions of dollars annually resulted

from advances in technology and customer service developed by AAAE's Transportation Security Clearinghouse (TSC) in its scant three years of existence.

Lori Beckman, A.A.E., security director at Denver International Airport, offered this assessment: "The TSC has been instrumental in decreasing the CHRC (criminal history records check) processing time and dramatically improving customer service. Another benefit is the TSC stores the fingerprint data submitted, which we will be able to use in the future for recurrent checks, thus eliminating the need to re-fingerprint employees."

Brian Thompson, operations director at Yuma (Arizona) International Airport, agreed, stating that, "Turnaround times on fingerprint submissions and results have decreased significantly over a short period of time, a testament to the success of the TSC."

The TSC was born in the aftermath of the September 11, 2001, terrorist attacks against the United States when FAA mandated that a criminal history records check be initiated on every individual employed in or applying for a position in secure areas of U.S. airports. Realizing that the Federal system in place at that time for conducting records checks—which took 52 days or longer to process fingerprint submissions—wouldn't meet the test, FAA signed an agreement with AAAE to facilitate fingerprint processing for aviation employees.

AAAE developed the TSC process over the past three years, using technical and administrative innovations that would save the aviation industry valuable dollars as well as time. Once established, the TSC was able to reduce the time it took for the aviation community to receive fingerprint results from months to an average of four hours, with most reports completed in 40 minutes.

Regardless of the size of airport, the TSC has enabled airport and airline employees to begin a new job or return to work quickly without delays caused by obtaining security clearances, thus virtually eliminating the problem of lost productivity. As Sgt. Carlos Garcia at San Antonio International Airport explained, "The entire staff at the TSC has always been able to provide answers and provide suggestions and solutions in a very timely manner to the multiple problems my office has encountered while attempting to comply with TSA (Transportation Security Administration) fingerprint requirements. The TSC has provided the logistics for the airports to comply with the TSA fingerprint mandate in a professional and very helpful manner."

Airlines as well as airports have been positive in their assessment of the TSC.

Darby James, senior manager-staffing administration for Continental Airlines, recalled the TSC's challenge: "They had the burden of bringing a flow to the process and there was very little room for error. It seemed the clearinghouse had taken on a responsibility they were not equipped to handle. The Air Transport Association held numerous conferences to discuss air carrier frustrations. In one conference, Continental requested a representative from AAAE attend and answer some of our questions and concerns. It was clear from this meeting that AAAE understood their responsibility and were working hard to make improvements. In 2002, we began seeing marked improvement from AAAE. They listened to our concerns, made improvements based on our suggestions and the process started to pick up speed. The time it takes to receive results has gone from nearly three months to 24 hours and in some cases, we receive results within hours. AAAE overcame a seemingly insurmountable task. Their efficiencies translate into millions of dollars in savings for the air carriers and airport operators."

Northwest Airlines said that, due to the TSC, the carrier has "significantly reduced our new employee processing costs and decreased the time it takes to perform one of our background checks." Southwest noted the TSC's successful efforts "to streamline and improve the fingerprint based criminal history record checks process." The carrier added that, "We have noticed a marked improvement in the turnaround time for receipt of CHRC results since the TSC took over as the fingerprint submission clearinghouse for airlines and airports."

In addition to significant improvements in fingerprint processing times, the TSC has one of the lowest per record error rates—2 percent compared with the 8 percent average Federal rate. This allows employees to keep on working, without the need for repeat trips to the badging office. Further, the TSC facilitated the first high-speed secure connection to the Federal fingerprint processing system and, through other technology improvements, allowed the TSA to lower electronic fingerprint processing prices to the aviation community. The TSC continues to work with TSA to offer the aviation industry even lower processing prices.

Effective and timely customer service by TSC employees helps to resolve mistakes made in fingerprinting at the airport or airline level before they turn into delays at the Federal level.

Laura Hoke, an airport security and public safety official at San Diego International Airport, offered the TSC staff praise for a "helpful attitude" and "prompt resolutions to our problems." In addition, Hoke stated, "You always take the time to be patient, help figure out what the problems are and get them resolved quickly. Your dedication to customer service is admirable."

THE TSC EXPLAINED

Created in December 2001, the Transportation Security Clearinghouse (TSC) provides one central location for managing the legally mandated task of checking the criminal history backgrounds of airport and airline employees. TSC established a quick and secure method for collecting fingerprints from more than 500 airports, airlines and other organizations across the country and transmitting them to the FBI for processing. TSC also collects user payments and provides customer service.

To meet the requirements outlined under the Aviation and Transportation Security Act and heightened demand related to aviation industry employee background checks, TSC:

- provides expedited processing and resolution of finger print-based and name-based checks through required federal channels;
- performs quality assurance checks on all inbound and outbound fingerprint submissions; and
- offers centralized billing tied to record submittals;
- allows regulated entities to submit fingerprints either electronically or on cards;
- ensures secure handling of investigation results;
- permits only air carriers and airports to view investigation results;
- provides accounting reconciliation services;
- facilitates access to training expertise, and assists the industry in purchasing; electronic fingerprinting equipment ; and
- facilitates resubmission of fingerprints for the regulated party.

TSC has taken a number of steps to make the process as easy and efficient as possible for the aviation industry. For instance, it created the first high-speed, secure connection to the federal fingerprint processing system and set up and brought online more than 500 separate submitting entities for fingerprint processing. TSC has handled more than 1.6 million fingerprint records, processing them and passing them on to the federal government in an average time of 16 minutes per record.

While aviation companies have benefited from the TSC's productivity advancements, commercial truckers who are applying for endorsements to carry hazardous materials (hazmat) are paying steep fees and taking weeks or months to obtain CHRC results, according to the American Trucking Associations (ATA).

Daniel England, CEO of C.R. England, Inc. trucking company, testified on behalf of the ATA at a May 11 hearing of the House Transportation and Infrastructure Subcommittee on Highways, Transit and Pipelines. "At a time when carriers are struggling to attract qualified drivers—and I want to emphasize that; it's one of the most serious problems we have—and freight volumes are up, TSA has imposed upon the industry an unwieldy fingerprint process that discourages drivers from obtaining hazardous materials endorsements," England told panel members.

England pointed to several failures in the process mandated for truckers:

- As of March 4, 2005, a month after the requirement had gone into effect for new applicants for hazmat endorsements, Illinois had submitted 644 fingerprint requests and received no responses from TSA;
- New York had submitted 350 fingerprint requests and received no responses;
- Vermont had submitted 10 fingerprint requests and received no responses;
- Iowa had submitted 138 fingerprint requests and received no responses;
- Mississippi had submitted 100 fingerprint requests and received zero responses;
- Kansas had submitted 150 fingerprint requests and received 40 responses;
- Florida had submitted 700 fingerprint requests and received 14 responses.

Several states are implementing the hazmat regulation unevenly, highlighting the problem with lack of uniformity, England stated. "Although the fingerprint requirement for renewals and transfers does not take effect until May 31, 2005, several states were stripping the hazmat endorsement from drivers who moved from one state to another, thus making them ineligible to haul hazardous materials loads until TSA processed the results of their background checks. Since a large number of carriers require drivers to have hazardous materials endorsements as a condition of work, these workers are eventually unable to work for a period of time," he said.

Although some of these problems have since been addressed, "It is unconscionable that these problems were allowed to detrimentally affect drivers' livelihoods and carriers' business for months after the program went into effect," England testified. "There are problems that the trucking industry still faces today that do not appear likely to be corrected in advance of May 31. In its analysis of its regulation, TSA estimated that there would be a 20 percent reduction in the number of drivers with hazardous materials endorsements. If the reduction is a result of individuals who are identified as threats being excluded from the transport of hazardous materials, then so be it. However, ATA cannot stand idly by if the reduction is attributable to a poorly designed process that dissuades drivers from seeking or renewing their hazardous materials endorsements. At a time of driver shortage, I would argue that the Nation's economy cannot afford this process to continue."

Todd Zinser, DOT deputy inspector general, told lawmakers at the same hearing that the TSC has completed more than 1.6 million fingerprint-based background checks since it began operations in January 2002. "While initially a concern, the issue of timeliness turned out to be a non-factor," Zinser said. "In that case, the American Association of Airport Executives served as a clearinghouse to facilitate the process of fingerprints for the airports and airlines. Since TSA is no longer part of the department, we do not have firsthand knowledge of how TSA is implementing the program or whether the experience at the airports provide any lessons to the hazmat endorsement rule," he added. But based on our observations at airports and airlines, strong cooperation among all stakeholders is absolutely critical to make the process efficient and effective."

The establishment of the TSC as the central location for processing and tracking fingerprint submissions also has resulted in numerous productivity enhancements that have allowed TSA to lower electronic fingerprint processing prices to the aviation community.

While hazmat truckers pay nearly $100 per person for fingerprint processing, Rep. Peter DeFazio (D-Ore.) pointed out that aviation industry employees using the TSC pay far less for more efficient processing. DeFazio told panel members that TSC "has more integrity and it's more efficient and they're apparently somehow either breaking even or making money on it at $29. And they're accessing the same database, which costs $22 so their processing cost is $7."

At another point in the hearing, DeFazio noted that the hazmat trucker background check "is a Federal certification for national security purposes." He asked, "Could we not go to a system like is being used in aviation, which works very well?"

For the future, the TSC has outlined plans to offer enhanced services to help the aviation industry meet its security challenges. In 2003, the TSC began offering Enhanced Background Screening Services (EBSS). Through EBSS, airports and airlines are able to verify the identity of individuals, complete criminal history checks, obtain driving records, and validate employment history, professional credentials, financial status and immigration status. These services have allowed airports and companies to answer questions about an individual's criminal history left unresolved by fingerprint checks done by the Federal Bureau of Investigation, as well as to examine other aspects of an individual's background relevant to assessing a job applicant's trustworthiness.

"TSC has developed a unique and enviable record of success in bridging non-Federal and Federal biometric-based background checks," said AAAE President Charles Barclay. "It has the processes, custom software and customer service focus needed for today's fast-moving work environment. TSC will not only continue to play a key role in CHRC for aviation workers, but will also be increasingly important for programs like Registered Traveler, TWIC and others that need to move forward and value speed," he said.

"AAAE, its members and its customers have made a significant investment to get this right for aviation, because the difference between months and hours for these checks has enormous implications for personnel costs in aviation," Barclay said. "We are eager to share the knowledge and systems we have carefully honed with other biometric credentialing programs in aviation and other industries."

Transportation Security Clearinghouse

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

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

In fact:

- The TSC process has reduced the time it takes for airports to get fingerprint results from an average of 52 days, pre-September 11, when submitting to OPM, to an average of 4 hours, with most reports completed in around 40 minutes. This reduction in time has enabled airports to put their employees on the job where they are needed, without the need to pull another valuable employee from their duties to serve as an escort. The TSC has *saved the industry hun-*

dreds of millions of dollars in productivity gains and employee retention as a result of reduced fingerprint check processing times.

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

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

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

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

The CHAIRMAN. Thank you very much.

Our next witness is Tim Sparapani—I hope I'm saying that right——

Mr. SPARAPANI. That's perfect.

The CHAIRMAN.—legal counsel for privacy rights, American Civil Liberties Union. Please.

STATEMENT OF TIMOTHY D. SPARAPANI, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

Mr. SPARAPANI. Good morning, Chairman Stevens, Co-Chairman Inouye, and distinguished Members of the Committee.

The ACLU, representing its 600,000 members, respectfully submits this testimony opposing Secure Flight and Registered Traveler.

It's time for Congress to decide that enough is enough. Secure Flight and Registered Traveler will not make us any safer, and they will certainly make us less free. Let me start with Secure Flight, and then turn to Registered Traveler.

For 4½ years, nearly 200 million wasted tax dollars, several name changes, and repeated unsuccessful modifications, Secure Flight is no closer to implementation today than when it was first proposed, shortly after 9/11. TSA's repeated failures to launch Secure Flight suggests this program should be abandoned.

While it seemed like a simple commonsense concept at first blush, attempts to implement Secure Flight demonstrated it is laden with unforeseen complexities, making it impractical, technologically difficult, and unlikely to improve our security. It also threatened civil liberties, and it's a poor use of limited security dollars compared to other options. Simply put, it's time to pull the plug.

Let's take one example: the redress procedure, which we've heard a little bit about this morning. No one questions the importance of establishing a procedure to help innocent Americans wrongly put on the "No-Fly" and "Selectee Lists" to get off, and stay off, the lists, yet, 4 years later, TSA still hasn't developed one.

If TSA cannot provide redress after 4 years, how can Congress have any confidence that TSA can build the rest of Secure Flight?

Secure Flight suffers from one critical security weakness. No matter how it's redesigned, Secure Flight will not stop a single terrorist from boarding an airplane, unless the terrorist tries to fly using their own name and documents. Unfortunately, as we all know, identity theft is all too common.

Security dollars are, unfortunately, limited, so we must spend wisely. Since Secure Flight can't make us safer, Congress needs to redirect TSA's energies to programs more likely to save lives. The hundreds of millions Secure Flight will cost should be redirected to more effective, straightforward security that has fewer complications for civil liberties, privacy, and the airlines. For example, many of your constituents might be surprised to learn that even now, not all carry-on bags, luggage, and cargo are screened for weapons and explosives. Congress should scrap these other programs and invest in new, narrowly tailored technologies to get this screening done.

Let me turn to Registered Traveler. Like Secure Flight, this concept seems commonsensical and appealing, at first blush. But, again, Registered Traveler opens up a snakes nest of complexities once you delve into rating Americans' riskiness and sorting them into categories about how trustworthy they are. And this program's security benefits remain unclear, because Registered Traveler cannot identify and stop terrorists who belong to a sleeper cell.

Every Registered Traveler supporter assumes that, of course, they will belong to the program. But, of course, some people will be denied, and other innocent Americans will be wrongly labeled too risky. No one, not Congress, not TSA, the companies pushing the program, or the ACLU, for that matter, knows the consequences for those wrongly denied participation. Will this create a third list of undesirable flyers, the "unregisterable travelers"? If so, will that list be used to automatically select someone for additional intrusive scrutiny every single time they try to fly, or to deny a security clearance necessary for a job, or to enter a government building? If companies wrongly determine that an applicant is risky, what legal recourse will applicants have to challenge that finding and its consequences?

Registered Traveler is flawed, from a security perspective, because no one knows what criteria will distinguish innocent travelers from a sleeper-cell terrorist awaiting instructions to attack. It's a flawed premise that, by checking a flyer's commercial data background, the Government or a company can identify terrorists.

Last fall, Congress decided commercial data was too often erroneous to be useful to prescreen passengers for Secure Flight. It was the right decision, and Congress should do the same thing for Registered Traveler by explicitly denying both TSA and participating companies commercial data to prescreen passengers.

In conclusion, since neither of these programs will provide the enhanced aviation security that proponents promise, this Committee should act now to prevent them being built at all, because they all pose unacceptable risks to civil liberties and personal privacy.

Extreme applications of either program that wrongly label an innocent American a risk could threaten a person's constitutionally protected, Supreme-Court-ratified right to travel. We urge Congress to revoke TSA's authorization for both programs. And let me reiterate that we're eager to work with you to make flying safer and consistent with our constitutional principles.

Mr. Chairman, this concludes my testimony, and I look forward to your questions.

[The prepared statement of Mr. Sparapani follows:]

PREPARED STATEMENT OF TIMOTHY D. SPARAPANI, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION

I. Introduction and Summary of Requests for Committee Action

The Honorable Chairman Stevens and Ranking Member Inouye, the American Civil Liberties Union ("ACLU"), representing its nearly 600,000 members, respectfully submits this testimony in opposition to the Secure Flight and Registered Traveler programs.

After four and one-half years, nearly $200 million wasted tax dollars,[1] several name changes, and repeated, unsuccessful reformulations of the underlying proposals, Secure Flight and Registered Traveler are no closer to implementation than when they were first proposed shortly after the tragic events of September 11, 2001. First introduced as CAPPS II and Trusted Traveler, Secure Flight and Registered Traveler remain predicated on the unproven, theoretical, and flawed premise that the government can predict whether an individual will at some future date commit a terrorist act. The Secure Flight Working Group, convened by the Transportation Security Administration ("TSA") to provide it with advice, concluded that " . . . there is not sufficient available intelligence to determine what characteristics indicate someone will be a threat." Secure Flight Working Group Rep., presented to the TSA, September 19, 2005, at 3. This premise, akin to alchemy and astrology

in its scientific accuracy, has led TSA to misdirect its resources towards establishing two passenger pre-screening programs that will not make us any safer but will make us less free. Attempts to establish these programs have served as massive diversions that to this day prevent TSA screeners from accomplishing their core mission. Congress can only draw one conclusion from the failure to build Secure Flight and the inherent weaknesses of Registered Traveler: authorizations for both programs must be terminated expressly, and Congress must force TSA to refocus on achieving its core mission by keeping known terrorists who are threats to aviation security off planes, and—for the first time—screening all carry-on bags, luggage, and cargo for weapons and explosives.

The ACLU requests that this Committee and Congress explicitly revoke authorization for both Secure Flight and Registered Traveler, no matter what they are called, and instead insist that the Department of Homeland Security's ("DHS") TSA focus its passenger pre-screening on accomplishing two goals: (1) paring the No-Fly and Selectee Lists maintained by the Federal Bureau of Investigation's Terrorist Screening Center ("TSC") down to known terrorists who personally pose a specific threat to aviation security only; and (2) simply comparing passenger manifest lists to this refocused list.[2]

If the TSA attempts to implement Registered Traveler, the ACLU requests that Congress expressly block the privatization of Registered Traveler and prevent the use of commercial data concerning applicants to determine whether a would-be flyer is qualified to sign up for Registered Traveler. Neither the government, nor companies should assign individuals a risk assessment based on commercial data, because the consequences of a wrongful determination could lead to many future deprivations of the exercise of rights and privileges. However, it is significantly more inappropriate to allow private companies to perform a governmental role to determine whether a passenger constitutes a threat and the Government still must act in a Constitutional manner, even if it has outsourced its responsibilities to the private sector. Companies cannot be trusted to make such determinations accurately. The consequences of such a negative determination would likely add the rejected applicant to a new third list—similar to the No Fly List or Selectee List—of undesirable flyers who are virtually certain to be subject to, at a minimum, extra scrutiny every time they attempt to fly, and, at worst, a permanent bar from flying altogether. As is discussed in greater detail below, this new third list of "Un-Register-Able travelers" would likely be shared with other Registered Traveler companies, the TSA, TSC, and, likely, other government agencies. Further, as Congress recognized last fall when it expressly prohibited the TSA from utilizing commercial data to prescreen passengers for Secure Flight, commercial data contains enormous error rates, is unreliable, and is not useful as a tool to predict whether a would-be flyer is a threat to aviation security.[3]

II. Secure Flight: A Dangerously Flawed Proposal that Should Be Terminated

Secure Flight, regardless of its form, permits unacceptable security weaknesses, while threatening civil liberties and personal privacy. It is hard to say for sure what Secure Flight will ultimately do since TSA has still not finalized a working plan, flow chart or business model for the concept. However, it appears that Secure Flight would:

1) Require TSA to gather passenger name record ("PNR") data from the airlines and travel agents who book tickets;

2) Require TSA to forward this information to the Federal Bureau of Investigation's Terrorist Screening Center ("TSC"), to compare the names of the ticket purchasers to those names on the No-Fly and Selectee Lists;

3) Require TSC to inform TSA whether a person attempting to fly is on either list; and

4) Require TSA to tell its airport screeners to (a) allow the person to fly unimpeded except for normal screening, (b) select the person for some additional and more intrusive screening, such as opening bags, patting the person down, screening for explosive residue, and/or detaining the person for questioning, or (c) inform the would-be passenger that their name is similar to that of someone on the No-Fly list and they are barred from flying.

While this concept appears easy to implement, it suffers from numerous and intractable problems.

A. Security Weaknesses Render Secure Flight Unwise

Secure Flight is fatally flawed from a security standpoint. To support Secure Flight, a person must accept the dubious premise that terrorists will attempt to

book a ticket and board a flight under their own names. This is a simplistic approach and one upon which we cannot allow our airline security to rely. Again, no terrorists will be prevented from boarding airplanes unless a terrorist both attempts to book a ticket and shows up to board a plane under his or her own name and documents. The ease with which identity theft and document fraud is accomplished renders this premise highly suspect, however. The U.S. Federal Trade Commission estimated in 2003 that "over a one-year period nearly 10 million people—or 4.6 percent of the adult population—had discovered that they were victims of some form of identity theft." Prepared Statement of the Federal Trade Commission before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate on Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, Deborah Platt Majoras, Chair of the Federal Trade Commission, March 10, 2005, available at *http://www.consumer.gov/idtheft/pdf/ftc—03.10.05.pdf*.

The intelligence community presumes that the Nation's enemies, such as Al Qaeda, are: (1) patient; (2) well-funded; (3) capable of committing identity theft with remarkable ease; and (4) capable of producing high-quality, forged identification documents that allow a terrorist to purchase tickets and present virtually undetectable papers under an assumed name. This programmatic weakness leads to what security experts dub False Negatives, an inability of Secure Flight to detect actual terrorists. If the system is not able to identify known terrorists, TSA's screening will have failed.

Again, the ACLU does not oppose the TSA vetting passenger lists against a narrowly constructed list of known terrorists who pose a specific threat to aviation security. If a wanted terrorist is foolish enough to fly under his or her own name, the government should immediately arrest the suspect or monitor the terrorist's activities while preventing the terrorist from committing acts of terror and violence.

The problem from a security and civil liberties perspective is that both the No Fly and Selectee Lists, which are at the heart of the Secure Flight proposal, are bloated with names of individuals who have absolutely no connection to terror and do not have the capability of threatening aviation security. This leads to numerous cases of False Positives, which distract TSA from finding the actual terrorists. False positive stories are ubiquitous. Each Senator who is a Member of this Committee likely has innocent constituents who have been unnecessarily harassed, delayed or outright denied the ability to fly. The ACLU has collected complaints from 1,000 of such constituents, 740 of which were gathered through our internet intake process, but we will highlight just four:

- Passenger David XXXXX (Aug. 16, 2005) was surrounded by armed police with guns drawn at the ticket counter when he was mistakenly identified as being on the No Fly List. Moreover, when he arrived at the gate, his checked luggage was brought to him, and he was forced to witness the search of his belongings at the gate, the whole process taking two hours.
- Passenger Gregory XXXXX (May 9, 2005), after having his luggage thoroughly searched, was separated from his five-year-old son who was hysterically crying and escorted into a private room where he was subjected to a cavity search and genital inspection. Gregory has been wrongly delayed overnight on five separate occasions and whoever is accompanying him is also subject to delays and searches.
- Passenger, Mary XXXXX (May 16, 2005) was forced by TSA screeners to be screened with a machine (Smiths Detection Ionscan Sentinel II), which she was told checked "to see if I have a bomb inside me." This machine photographed her and TSA denied her repeated requests to view the picture or be provided a copy.
- Passenger Hussein XXXXX (July 23, 2005) is a Lebanese citizen who has been a legal resident of the U.S. since 1992. During his layover in Minneapolis, Minnesota while flying from Lebanon to Seattle, Washington, he was escorted off the plane by five security officers to a room away from the gate. He was questioned about his family, extended family, how he files taxes, his business, his real estate holdings and so forth. Additionally, the officers demanded he give them access to his computer, which he initially refused because it contained confidential information about his clients. After five hours of interrogation, he was exhausted and delirious so the officers gave him a choice of either being detained overnight and being questioned the following day or having an appeal inspection in Seattle. He was scheduled to appear at the U.S. Customs and Border Protection Office in Seattle on July 25, 2005. In the past, he has had similar experiences. For example, on October 3, 2004, he was stopped in Portland, Oregon on his way to Frankfurt, Germany by U.S. Customs who interrogated him.

He was given no medical attention when he fainted, and security officers laughed at him while they waited until he regained consciousness.

At least four Members of Congress—the Honorable Senator Ted Kennedy (D–MA), and the Honorable Congressmen Darrell Issa (R–CA), John Lewis (D–GA) and Don Young (R–AK)—have names similar to those of individuals on those bloated Lists. The Honorable Congresswoman Zoe Lofgren (D–CA) reported in Congressional hearings last summer that her husband has been repeatedly selected for additional security screening. Nuns and infants have been found on the No Fly List. To be effective, the Lists must be paired down only to known terrorists—not criminals, not deadbeat dads, not drug dealers. The advice provided by an independent panel of experts to the Department of Homeland Security concurs:

Secure Flight should be narrowly focused.

TSA should limit Secure Flight's mission to correctly identify individuals in the traveling public who are on the Do Not Fly and Selectee lists. The case has not been made for any expansion of the mission of Secure Flight beyond identification of individuals on those lists.

Department of Homeland Security Data Privacy and Integrity Advisory Committee: Recommendation on the Secure Flight Program Rep., Adopted Dec. 7, 2005, at 2 (emphasis in original). Limiting the names on the list is the only way that TSA can focus on its core mission: preventing another terrorist attack on an airplane. Senator Kennedy (D–MA) revealed at a Senate hearing that due to the fact an "E. Kennedy" was on the No Fly List, Senator Kennedy repeatedly was selected for additional screening. Every minute spent treating Senator Kennedy like a potential terrorist is one less minute that could be spent catching the next Mohammed Atta.

B. Civil Liberties: Secure Flight Leads to a Denial of the Right to Travel in Extreme Cases and Leads to Racial Profiling

In addition to being fatally flawed from a security standpoint, Secure Flight also is flawed from a civil liberties standpoint. First, using a bloated No Fly List to prevent innocent people from flying wrongly deprives them of their constitutionally protected Right to Travel. The United States Supreme Court has stated that:

> The word "travel" is not found in the text of the Constitution. Yet the "constitutional right to travel from one State to another" is firmly embedded in our jurisprudence. *United States* v. *Guest*, 383 U.S. 745, 757, 86 S.Ct. 1170 (1966). Indeed, as Justice Stewart reminded us in *Shapiro* v. *Thompson*, 394 U.S. 618, 89 S.Ct. 1322 (1969), the right is so important that it is "assertable against private interference as well as governmental action . . . a virtually unconditional personal right, guaranteed by the Constitution to us all." *Id.*, at 643, 89 S.Ct. 1322. (concurring opinion).

Saenz v. *Roe*, 526 U.S. 489, 498–99 (1999). We suspect that TSA will soon begin to apply the Secure Flight concept to those who travel by train, interstate bus, boat and ferry. Some Americans living in remote regions of Alaska, or on the islands of Hawaii and Puerto Rico simply cannot drive to conduct their business, so the consequence for someone who is wrongly put on the No Fly List is severe and could force them to move to conduct their daily affairs. [4]

Second, as too many Americans have experienced, people who are wrongly put on either list have no guarantee that they will be able to ever get off and stay off the lists. Establishing a transparent, workable redress procedure to help people wrongly listed should have been the first and easiest thing TSA accomplished. TSA has provided numerous promises that such a redress process would be provided but, to date, has still not accomplished this goal:

- "CAPPS II will include a comprehensive redress process for those passengers who have questions concerning their experience. TSA will appoint an Ombudsman to handle any inquiries. These capabilities will result in improved resource scheduling and other operational efficiencies." (March 7, 2003) Congressional briefing by Ben H. Bell, III, Dir. Office of National Risk Assessment ("ONRA") TSA, available at *http://www.acte.org/initiatives/CAPPS_II_CongressBriefing.pdf*.
- "CAPPS II will also include a comprehensive redress process for passengers. TSA will appoint a Passenger Advocate to work with our current Ombudsman program, to handle any inquiries or complaints raised by passengers with regard to the CAPPS II system. Where a passenger—of any nationality—believes that he or she is being improperly singled out for heightened scrutiny, this will be the place for this passenger to turn to have his or her concerns addressed. This is more than a matter of fairness—because CAPPS II is also a resource

allocation tool, it is in TSA's interest to know where we are making mistakes. The Passenger Advocate will thus not only promote fairness and privacy and passenger confidence, but system effectiveness and efficiency." (May 6, 2003) Statement of Stephen McHale to the European Parliament, Dep. Admin., TSA, available at *http://www.europarl.eu.int/comparl/libe/elsj/events/hearings/20030506/mchale_*speech.pdf.

- "The redress system is based on having an ombudsman and a passenger advocate designated and a process in place so that when an individual finds that they are being repeatedly selected as a secondary screenee during their transit through the airport that they will have an opportunity then to contact TSA, the ombudsman, and the passenger advocate and then we will have the capability to have a decision made at the TSA level concerning going in on that individual and then adjusting the criteria for that individual after we verify their name, date of birth, address to [sic] for into that and make these decisions, we think, in a rapid matter so that it is not a bureaucratic system of waiting forever to get a response. Our goal is to have a redress system that has flexibility in it and speed and scratches the itch for the traveling public regarding frustrations over being selected repeatedly." (March 17, 2004) David M. Stone before House of Representatives Transportation Committee, Subcommittee on Aviation, available at *http://www.house.gov/transportation/aviation/03–17–04/stone.pdf.*
- "In addition, the new program [Secure Flight] will also include a redress mechanism through which people can resolve questions if they believe they have been unfairly or incorrectly selected for additional screening." (August 26, 2004) TSA Press Release, available at *http://www.tsa.gov/public/display?theme=44&content=09000519800c6c77.*
- "Before implementing a final program, however, TSA will create a robust redress mechanism to resolve disputes concerning the Secure Flight program." (June 17, 2005) Lisa S. Dean, TSA Privacy Officer, Secure Flight Test Phase Privacy Impact Assessment, available at *http://www.tsa.gov/interweb/assetlibrary/Secure_*Flight_SORN_PIA.pdf.
- "In conjunction with the Secure Flight program, TSA has charged a separate Office of Transportation Security Redress to further refine the redress process under the Secure Flight program. The redress process will be coordinated with other DHS redress processes as appropriate. Utilizing current fiscal year funding, resources have been committed to this Office to enable it to increase staffing and to move forward on this important work. TSA recognizes that additional work remains to ensure that there is a fair and accessible redress process for persons who are mistakenly correlated with persons on the watch lists, as well as for persons who do not in actuality pose a security threat but are included on a watch list. (June 29, 2005) Statement of Secure Flight Assistant Administrator Justin Oberman to House of Representatives Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, available at *http://homeland.house.gov/files/TestimonyOberman.pdf.*

Yet, four and one-half years later, TSA has still not managed to accomplish this goal. Congressional frustration over this failure led, in part, to the express requirement codified in both the FY 2005 and 2006 DHS Appropriations bills, Pub. L. No. 108–774 §522(a), (d)–(f) (2004)[5] and Pub. L. 109–90 §518(a)–(b) (2005)[6] that the Government Accountability Office ("GAO") certify the establishment of a working, fair redress procedure before Secure Flight can be implemented. As the GAO's March 28, 2005 report regarding Secure Flight stated, TSA has failed to accomplish even this simple matter. U.S. Government Accountability Office Rep., Aviation Security, Secure Flight Development and Testing Under Way, but Risks Should be Managed as System is Further Developed ("GAO Report"), March 28, 2005, at 1. Just three weeks ago, DHS Secretary Chertoff and Secretary of State Rice issued a joint statement pledging the rollout of a workable redress process. "'*One Stop' Redress for Travelers.* Sometimes mistakes are made. Travelers need simpler ways to fix them. Therefore, DHS and State will accelerate efforts to establish a government-wide traveler screening redress process to resolve questions if travelers are incorrectly selected for additional screening." Rice-Chertoff Joint Vision: Secure Borders and Open Doors in the Information Age. Department of Homeland Security, Department of State: Joint Press Release, Jan. 17, 2006, available at *http://www.state.gov/r/pa/prs/ps/2006/59242.htm* (emphasis in original). As too many Americans have experienced, and reported to the ACLU, the "passenger identity verification form" process TSA now utilizes is inadequate and does not guarantee that passengers will not be delayed or denied when trying to fly in the future. As the GAO reported, ". . . the effectiveness of the current redress process is uncer-

tain," and "[t]he draft redress process documentation does not address a means for passengers who are inappropriately denied boarding to seek redress." GAO Report at 56, 58. Thus, people whose names are wrongly added to the lists—or, more likely, have names similar to others on the Lists—are perpetually doomed to—at best—unnecessary harassment, embarrassment and delays every time they fly. At worst, they will be denied the ability to fly at all. Congress should ask: If TSA cannot build a redress process after nearly four and one-half years for Secure Flight to prevent against civil liberties violations, how can TSA be trusted to build an effective, civil liberties-respecting passenger pre-screening program?

Secure Flight will likely lead to impermissible racial profiling. The names most likely to be on the No Fly and Selectee Lists that will be utilized for Secure Flight are likely to be those of Muslims, or people of Arab or Middle Eastern dissent. Thus, a disproportionate number of people who are wrongly selected for additional screening or barred from flying outright will be those of these classes. Congress must guard against allowing a program designed to increase security from becoming a tool for racial profiling. Such profiling wastes precious resources and ignores the fact that the next terrorists may draw from those demographics that are the majority races, religions or ethnic backgrounds in this country.

C. Privacy: TSA's Failures to Safeguard Personal Data for Secure Flight Unacceptably Threaten Personal Privacy

As demonstrated by the tortured attempts to test the viability of CAPPS II and Secure Flight, Secure Flight, if implemented, unacceptably threatens personal privacy. Testing of Secure Flight has led to two high profile and massive privacy violations. In 2003, JetBlue Airways gave 5 million actual passenger itineraries to Torch Concepts, a Defense Department contractor, which was attempting to study whether the government could prescreen passengers to determine who was a high-risk customer. Bruce Mohl, "Airlines Weigh Privacy Issues," *Boston Globe*, Oct. 12, 2003. In a separate incident last summer, the GAO reported that TSA had violated the Privacy Act of 1974, Pub. L. No. 93–579 (1974), codified at 5 U.S.C. §552, by giving personally identifiable information on millions of people without giving legally required public notice. As stated by Senators Collins and Lieberman in a July 22, 2005 press release and letter to Secretary of the U.S. Department of Homeland Security Michael Chertoff, the GAO reported that "TSA failed to comply fully with the Privacy Act when it 'collected and stored commercial data records even though TSA stated in its privacy notices that it would not do so.'" That letter further stated that a private contractor had "obtained more than 100 million records from commercial data aggregators in violation of the Privacy Act." Senators Collins and Lieberman Criticize TSA for Violating Privacy Laws While Testing Passenger Prescreening System: GAO Findings Conclude TSA Failed to Comply with the Privacy Act, July 22, 2005, available at *http://hsgac.senate.gov/index.cfm?Fuseaction=PressReleases.Detail%PressRelease—id=106.*

Further, TSA has not learned from its privacy breaches; it has not yet even fully assessed the impact of implementing Secure Flight on passengers' personal privacy despite a Congressional mandate. The GAO's report regarding Secure Flight concluded that "TSA has not yet clearly defined the privacy impacts of the operational system or all of the actions TSA plans to take to mitigate potential impacts." GAO Report, at 1. If past experience is the best guarantee of future performance, TSA cannot be trusted with the sensitive, private data it will demand from each passenger. The inability of the TSA to adequately safeguard sensitive, personally identifiable information about actual passengers during testing of the program's efficacy and viability provides no assurance that should the program be implemented each passenger's information will be safeguarded. Indeed, if Secure Flight is implemented, the personal information of 1.8 million passengers on 30,000 flights will be electronically transferred from airlines and ticketing companies to TSA and TSC every single day. This will lead to numerous data breaches that dump sensitive information into the public sphere. For identity thieves, it will be like taking candy from a baby.

D. Track Record of Failure: Past TSA Failures Suggest Future Launch Efforts Will Not Be Better for Secure Flight

Regardless of the security, civil liberties and privacy risks raised by what TSA's public statements concerning Secure Flight suggest, the program remains wholly conceptual more than four years after passage of the Aviation and Transportation Security Act, Pub. L. No. 107–71 (2001), that authorized its creation. Slippage of deadlines has been the rule for Secure Flight and its predecessor CAPPS II:

- "TSA expects to test CAPPS II this spring and implement it throughout the U.S. commercial air travel system by the summer of 2004." TSA Press Release,

March 11, 2003, available at *http://www.tsa.gov/public/display?theme=44&content=09000519800193c2.*

- "Of note, the terrorist screening center remains on schedule to bring the first version of the consolidated terrorist screening database on line by March 31, 2004, and achieve full operation capability by the end of the year." Testimony of David M. Stone, before Hearing of House of Representatives Comm. on Transportation, Subcomm. on Aviation on status of CAPPS II, March 17, 2004, available at *http://www.house.gov/transportation/aviation/03–17–04/stone.pdf.*
- "'We're in great shape as we enter the testing phase' of the program, Oberman said. He said if all goes according to plan, the new system will go into operation in late spring or early summer of 2005." Wash. Post, Nov. 13, 2004, available at *http://www.washingtonpost.com/wp-dyn/articles/A46610–2004Nov12.html.*

Every review by a government agency or independent commission in the last year found Secure Flight to be woefully undefined because of the myriad conceptual and practical flaws, no matter how the program is modified.

- On March 28, 2005, the GAO summarized "TSA's Status in Addressing Ten Areas of Congressional Interested included in Public Law 108–334," finding that TSA had only achieved one of the ten requirements—establishing an internal oversight board—and had not yet even finalized a "draft concept of operations." GAO Report, at 4.
- On September 19, 2005, TSA's Secure Flight Working Group concluded that:

  Congress should prohibit live testing of Secure Flight until it receives . . . a written statement of the goals of Secure Flight signed by the Secretary of DHS that only can be changed on the Secretary's order. Accompanying documentation should include: (1) a description of the technology, policy and processes in place to ensure that the system is only used to achieve the stated goals; (2) a schematic that describes exactly what data is collected, from what entities, and how it flows through the system; (3) rules that describe who has access to the data and under what circumstances; and (4) specific procedures for destruction of the data.

Report of the Secure Flight Working Group, Presented to the TSA, September 19, 2005, at 32.

- In August 2005, the Department of Justice's Inspector General issued a report, which said that TSC could not plan to assist in Secure Flight because TSA failed to even establish a working flow chart for Secure Flight. "The TSC's difficulties in estimating the costs for Secure Flight are exacerbated by the TSA's failure to specifically define the scope of each implementation phase. As a result, the TSC has been unable to adequately project its resource requirements for responding to the expected increase in workload." Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program, U.S. Department of Justice Office of the Inspector General, at (ix). Further, the report concluded that " . . . TSC is trying to plan for a program that has several major undefined parameters. Specifically, the TSC does not know when Secure Flight will start, the volume of inquiries expected and the resulting number of resources required to respond, the quality of data it will have to analyze and the specific details of the phased-in approach for taking the program from 'pre-operational testing' in September 2005 to full operational capability in FY 2007." *Id.* at (ix).

On December 7, 2005, a panel of independent experts advising DHS found that " . . . the program is not yet fully defined . . . " and recommended that " . . . there must be an overall system description that addresses all aspects of the Secure Flight system including external supporting systems, policies, applications and infrastructures, as well as related business processes managed by entities external to the Secure Flight program office." Department of Homeland Security Data Privacy and Integrity Advisory Comm. Rep., Recommendation on the Secure Flight Program, Adopted Dec. 7, 2005, at 1, 2.

As the ACLU stated at the outset, this program—like Registered Traveler—is a moving target, which leads to only one conclusion: the testing thus far has been unable to demonstrate that Secure Flight can predict those flyers who are potential terrorists and/or identify and prevent known terrorists from flying. No modification can change the conclusion that Secure Flight simply will not work, the ACLU recommends that Congress:

1) Direct the TSC only to maintain a short list of known terrorists who pose a specific threat to aviation security and dispense with the bloated No Fly and Selectee Lists.

2) Explicitly repeal the authorization for Secure Flight or any similar program, and, instead, use TSA and TSC to compare names of would-be passengers to the pared down list of known terrorists who pose a specific threat to aviation security.

3) Utilize the funds saved by eliminating Secure Flight to invest in programs that will greatly enhance physical screening including the introduction of appropriate new technologies and the screening of all carry-on bags, luggage and cargo for explosives and weapons.

4) If Congress decides to allow Secure Flight testing to continue, it should insist that TSA comply with the spirit and letter of the law expressed in both the FY 2005 and FY 2006 DHS Appropriations laws. Congress should insist expressly that TSA not implement the program, even on a test basis impacting actual passengers, unless and until the GAO certifies first that all ten of the Congressionally mandated criteria have been satisfied.

III. Registered Traveler: The Misalignment of Profit and Security Trades the Promise of Speed for Personal Privacy and the Illusion of Enhanced Security

Like Secure Flight, TSA's proposed Registered Traveler program should be blocked from implementation. The Registered Traveler concept, whether entirely government run or partially privatized, trades the promise of speedy screening for the illusion of enhanced security. This concept misaligns the profit motive with the country's need for safety. The ACLU does not believe that security should be traded for expediency. The ACLU therefore recommends that Congress eliminate TSA's authorization to develop Registered Traveler. If Congress does proceed with Registered Traveler, the ACLU recommends that TSA not privatize Registered Traveler. If Congress does allow TSA to privatize Registered Traveler, the ACLU recommends that the government—not commercial companies—undertake background checks on program applicants, and that Congress expressly prohibit private companies from accessing third-party companies' commercial data to determine applicants' risk assessments.

Registered Traveler also remains largely undefined, but the TSA's public pronouncements suggest the basic parameters of the program. Frequent flyers would be granted some combination of alternating security screening benefits, which would induce them to undergo an extensive background check to pre-clear them for flying. Passengers would be required to provide extensive amounts of sensitive, personally identifiable information to qualify. The information provided is likely to include, but not be limited to, financial and credit information, residence history, and biometrics such as an iris scan or fingerprint. If the background check—either undertaken by the government or a private sector company—raises no red flags, the applicant would either (depending on the airport) be permitted to cut to the front of the security screening lines (as has been done in the Orlando, Florida pilot program), or would be ushered into a screening lane dedicated solely for Registered Traveler participants.

A. Security: Registered Traveler Wrongly Assumes Background Data can Predict a Person's Future Behavior

Like Secure Flight, Registered Traveler rests on a dangerously flawed premise, which causes it to provide the illusion of greater security without actually making airlines safer. Registered Traveler will be vulnerable to "sleeper cells," *i.e.*, terrorists with no previously known or detectable ties to terror who could establish themselves as unremarkable members of society. To support Registered Traveler, one must accept the untested premise that by checking a would-be flyer's background, the government (or a commercial enterprise) can identify terrorists and predict a flyer's future behavior. This premise is fatally flawed. The data that will be provided for a background check may allow a credit card company to determine whether a person is a credit risk, but it cannot identify someone harboring a dangerous plan and a willingness and capability to undertake a terrorist attack that causes a threat to aviation. No one knows what criteria will allow the government to ferret out the innocent traveler from the sleeper cell participant waiting for instructions to carry out a terrorist attack. For example, the four men who bombed the London, England subway system on July 7, 2005 reportedly had no prior known ties to terror. Thus, no amount of data could have uncovered their sympathies or plans. Similarly, the 9/11 terrorists spent many months in this country, demonstrating that Al Qaeda is

patient and well funded. Congress should expect that similar cells of innocent-seeming individuals could be sent to this country to establish lives that would allow them to pass the Registered Traveler background checks. This would allow them to avoid suspicion until they later receive instructions to conduct terrorist attacks. Because glaring loopholes exist in the Nation's physical screening, no amount of "layered security" will detect these sleeper cells.

Further, while background checks look at people's data histories, they only provide a review at one moment in time. Thus, they cannot predict future behavior. Simply because a person has not, to date, demonstrated indicia of adherence to a dangerous ideology does not mean that a person's ideology will not evolve. No one could have predicted the rapid transformation of John Walker Lindh from college student to disgruntled Taliban fighter. Further, TSA must not focus solely on Al Qaeda. Lone, disgruntled individuals may lose their minds and some may attempt to commit a terrorist attack on aviation. If that person has previously been an upstanding member of society, there would be nothing to prevent them from participation in Registered Traveler and its lessened security screening.

B. Privatization of Registered Traveler is Dangerous: Registered Traveler Misaligns Profit Motive with Security

Registered Traveler will make Americans less safe because it misaligns profit incentives with the national security needs of this country. Corporations exist to make profit for their owners and shareholders. That legal reality creates an incentive to optimize and cut corners where possible. Thus, privatization of such a program will make us less safe in two different ways.

First, to attract participants, companies will offer the fastest possible screening lanes, while maximizing profits. This will require hiring low-cost, low-skill laborers who will go through the motions of screening Registered Traveler participants for weapons and explosives. The government's TSA screeners already routinely fail to identify such dangerous contraband during routine testing. Private screeners, overseen by managers who are intent on maximizing the attractiveness of the Registered Traveler screening lanes, will have a disincentive to go the extra mile to identify items that could bring down a plane or harm the crew and passengers; doing so slows down screening and eliminates the one advantage for participants. Furthermore, the same company will take applications for Registered Traveler, conduct the background checks on applicants, gather the biometric data to issue pass cards, and then may perform screenings at the airports. This streamlined, profitable vision does not provide for sufficient security oversight. If a terrorist fools the one company the terrorist applies to, the terrorist will be given a Registered Traveler pass providing them with reduced physical screening at the airport every time they attempt to fly.

Second, offering "advantages" to decrease screening time per flyer, such as those TSA has publicly promised—*i.e.*, not forcing individuals to have their shoes, jackets and laptop computers screened—creates vulnerabilities. If there is a security value in screening for these items, then all flyers—whether they are in the regular screening lanes or the dedicated Registered Traveler screening lanes—should be forced to comply. Congress should expect that Al Qaeda or other enemies of this Nation will detect the weaker security protocols for Registered Travelers and will attempt to exploit them to carry out future attacks.

C. Civil Liberties: Reliance on Flawed Commercial Data Leads to the Wrongful Placement on a List of Un-Register-able Travelers with Unknown Consequences

Registered Traveler also impermissibly threatens civil liberties. The background checks will rely on commercial data, which is notoriously inaccurate. Data errors are common in every database. Numbers and names get transposed. While there can be only one Senator Ted Stevens, data about people with similar names, like T. Stevens, Teddy Stevens or Theodore Stevens could be wrongly merged with the Senators files collected by various companies.[7] The data aggregators who are most likely to provide the commercial data, like ChoicePoint, do not audit the accuracy of their dossiers of information. Thus, either the government or a private company will assign a risk assessment to Registered Traveler applicants that could be fundamentally wrong. Current law does not give consumers the right to access, review, and correct errors in files maintained by commercial enterprises.

In the fall of 2005, Congress decided this risk was unacceptable and passed a law expressly prohibiting TSA from using commercial data to pre-screen passengers for Secure Flight. Congress codified this understanding in the FY 2006 Department of Homeland Security Appropriations bill. During the Senate Appropriations Committee's mark-up of the bill, Ranking Member Robert Byrd (D–WV) said that:

> . . . the bill contains an important protection for the privacy rights of Americans. We need always to keep these rights in mind. I thank Chairman Gregg for his support of language that I recommended concerning Secure Flight, the Department's proposed new airline passenger profiling system. The language would prohibit the use of commercial databases for confirming the identity of airline passengers. **Such commercial databases are unreliable and potentially invade people's privacy.**

Transcript of Senate Appropriations Committee Mark of H.R. 2360, the FY 2006 DHS Appropriations bill, July 7, 2005 (emphasis added). On January 20, 2006, TSA demonstrated that it did not get the message when it announced that the newly reformulated Registered Traveler program would have private companies screen data collected by other private companies concerning applicants. The ACLU, therefore, requests that Congress again expressly prohibit by statute TSA—or companies with which TSA contracts to perform Registered Traveler services—from utilizing commercial data to assess applicants for Registered Traveler.

No one—not Congress, TSA, the companies wishing to operate Registered Traveler programs, or the ACLU—knows what it will mean for someone to be wrongly denied when they apply for Registered Traveler. If a third list of Un-Registerable Travelers is created from those blocked from joining Registered Traveler, there may be other consequences such as that list being used to deny the applicant a government security clearance necessary for a job, or to prevent the applicant from entering a government building. Several questions about the consequences should be considered:

> 1) Will those denied registration be put into a third list of undesirable flyers—the "Un-Registerable Travelers?"
>
> 2) If so, will they be automatically selected for additional, intrusive screening every single time they fly?
>
> 3) If private companies, essentially functioning as government actors, wrongly determine that an applicant poses a risk, what legal recourse will the flyer have to challenge that finding if it is used to create a third list?

Moreover, those denied the chance to be Registered Travelers will be forever required to pass through the "slow" screening lanes for all flyers. There, they will be subjected to more invasive screening than the Registered Travelers. Finally, those denied are likely to be disproportionately poor, minorities, and women; these groups simply are less likely to have the lengthy data trail and credit standing to guarantee participation. Congress will need to ensure that this program cannot create a *de facto* second-class status for would-be flyers whose commercial data is not as clean as that of wealthy businessmen.

D. Privacy: Frequent Travelers Should Not be Forced to Choose Between their Sensitive, Private Information and Speed of Screening

Registered Traveler also poses an unacceptable inducement that causes business and other frequent travelers to involuntarily forego their personal privacy for the promise of speed and efficiency in screening. This is a choice that Congress should not ratify. No one should be forced to choose between privacy and speed. When screening lanes are taken from the mass of the flying public and dedicated for Registered Travelers, the lines for everyone else get significantly longer. This creates a scarcity of time and screening lanes. Inevitably, the occasional traveler or privacy-sensitive traveler will be induced to undergo extensive background checks and share their most sensitive, personally identifiable information to migrate to the faster lanes. Given a truly equal choice, almost no one would voluntarily share his or her private information. But when the TSA turns screening into a chokepoint at airports, it forces people to override their instincts. This enforced scarcity renders the choice to share private information involuntary.

E. Speed and Efficiency Benefits Negligible, Unproven and Possibly Illusory

Ironically, the benefits of participation in Registered Traveler remain unclear and will likely prove illusory as the program grows and increasing numbers of people are registered for the "fast lane." To date, the TSA has not published any studies demonstrating that either dedicating screening lanes for Registered Traveler participants, or allowing Registered Traveler participants to jump to the front of the line, will not make the lines for the mass of the flying public longer. A small percentage of frequent flyers constitute a disproportionate percentage of the individual screening interactions. Therefore, simply removing them from the "slow" screening lines will not necessarily translate into faster screening lanes for Registered Travelers. If we assume that the vast majority of all the targeted frequent flyers participate, then the dedicated lines for Registered Travelers will be lengthy at peak flying

times. During off-peak hours, the lines are not likely to be long in either the normal screening lanes or the Registered Traveler lanes. Similarly, some airports do not experience the lengthy lines that would push people to apply for Registered Traveler. Finally, TSA promises to occasionally modify the screening protocols for Registered Travelers to avoid predictability by terrorists. This will erode or eliminate any of the already negligible speed and efficiency gains and it does little for frequent flyers eager to fly during peak hours. The ACLU, therefore, wonders how TSA can guarantee Registered Traveler participants any benefits at all.

The ACLU recommends that Congress expressly eliminate the authorization for Registered Traveler and ensure that all flyers be treated efficiently during screening. The ACLU further recommends that Congress utilize the funds saved to redesign some airports to permit for more screening lanes to be used by all flyers, purchase more screening equipment and hire more TSA screeners.

IV. Conclusion: Secure Flight and Registered Traveler are Not Ready for Take Off and Congress Must Take Action

The ACLU has shown that Secure Flight and Registered Traveler pose unacceptable risks to security, civil liberties and privacy. For too long, TSA has wasted money attempting to launch programs predicated on a flawed assumption that a flyer's behavior can be predicted by reviewing information collected about their past. Since TSA cannot demonstrate the benefits of these programs Congress should:

- Expressly eliminate the statutory authorization for TSA to test and implement these programs, irrespective of the programs' names.
- Request that the TSC scrap the bloated No Fly and Selectee Lists and instead maintain a pared down list of known terrorists who pose a specific threat to aviation security. TSA and TSC should then be directed to compare passenger manifest lists to the names of those terrorists who buy tickets and attempt to fly under their own names.
- If Congress permits Registered Traveler to proceed, Congress should insist that it be solely government run and operated.
- If Congress insists that Registered Traveler be partially privatized, it should prohibit expressly Registered Traveler companies, or any companies performing background checks, from utilizing commercial data about applicants obtained from other companies.

ENDNOTES

[1] During Fiscal Years 2002 through 2006, Congress has appropriated a total of $162.3 million for the combined CAPPS II and Secure Flight program, and $30 million for Registered Traveler. The Presidents' FY 2007 budget requests an additional $40 million for Secure Flight.

[2] The ACLU does not oppose the Federal Government's keeping and maintenance of a list of terrorists known to pose a threat to aviation security. Keeping such a list, limited only to known terrorists, focuses the Nation's anti-terror efforts to prevent against another attack on a passenger airline. Coupling a refocused list with (1) improved physical screening of all carry-on bags, luggage and cargo; and (2) the introduction of new technologies that are narrowly tailored to search for threats such as plastic explosives which cannot be detected by current metal detectors, will substantially improve the safety of domestic commercial air flights, while eliminating infringements on civil liberties and privacy. Where, in the rare instance, people attempting to fly have names similar to such known threats to aviation security, TSA and TSC could request the submission of the bare minimum of additional personally identifiable information—such as three part name and date of birth—that will distinguish innocent travelers from terrorists. TSA and TSC also should be forced to provide a means for permanently removing these innocent people from suspicion, perhaps through the government's provision of a unique identifier.

[3] *See,* H.R. Conf. Rep. No. 109–241, at 54 (2005). ("The provision also prohibits the use of commercial data."); and Pub. L. No. 109–90 §518(e), ("None of the funds provided in this or previous appropriations Acts may be utilized for data or a database that is obtained from or remains under the control of a non-Federal entity: Provided, That this restriction shall not apply to Passenger Name Record data obtained from air carriers.").

[4] The ACLU fears that unless Congress acts, the principle of information sharing will lead to the migration of the No Fly and Selectee Lists to other government agencies, which may use the lists to wrongly deny innocent individuals access to government buildings. It would be unacceptable for these Lists, which should be used only to find and stop those who threaten aviation, to be used to prevent innocent people from accessing government buildings. Members do not want veterans

wrongly denied access to Veterans Affairs offices or senior citizens wrongly denied access to Social Security Administration buildings. Furthermore, circulation of these lists—once pared down to one list consisting solely of those known threats to aviation security—make it far more likely that terrorists will know the government is looking for them by name. Thus, national security concerns suggest that the revised List be kept close and used only for passenger pre-screening. Therefore, the ACLU recommends that Congress should explicitly mandate that the No Fly and Selectee lists not metastasize and migrate to be used by other Federal, State and local governments.

[5] Section 522 provides in pertinent part:

(a) None of the funds provided by this or previous appropriations Acts may be obligated for deployment or implementation, on other than a test basis, of the Computer Assisted Passenger Prescreening System (CAPPS II) or Secure Flight or other follow on/successor programs, that the Transportation Security Administration (TSA), or any other Department of Homeland Security component, plans to utilize to screen aviation passengers, until the Government Accountability Office has reported to the Committees on Appropriations of the Senate and the House of Representatives that—

(1) a system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights by the TSA may appeal such decision and correct erroneous information contained in CAPPS II or Secure Flight or other follow on/successor programs;

(2) the underlying error rate of the government and private data bases that will be used both to establish identity and assign a risk level to a passenger will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted;

(3) the TSA has stress-tested and demonstrated the efficacy and accuracy of all search tools in CAPPS II or Secure Flight or other follow on/successor programs and has demonstrated that CAPPS II or Secure Flight or other follow on/successor programs can make an accurate predictive assessment of those passengers who may constitute a threat to aviation;

(4) the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which CAPPS II or Secure Flight or other follow on/successor programs are being developed and prepared;

(5) the TSA has built in sufficient operational safeguards to reduce the opportunities for abuse;

(6) substantial security measures are in place to protect CAPPS II or Secure Flight or other follow on/successor programs from unauthorized access by hackers or other intruders;

(7) the TSA has adopted policies establishing effective oversight of the use and operation of the system;

(8) there are no specific privacy concerns with the technological architecture of the system;

(9) the TSA has, pursuant to the requirements of section 44903(i)(2)(A) of title 49, United States Code, modified CAPPS II or Secure Flight or other follow on/successor programs with respect to intrastate transportation to accommodate States with unique air transportation needs and passengers who might otherwise regularly trigger primary selectee status; and

(10) appropriate life-cycle cost estimates, and expenditure and program plans exist.

(d) None of the funds provided in this or any previous appropriations Act may be utilized to test an identity verification system that utilizes at least one database that is obtained from or remains under the control of a non-Federal entity until TSA has developed measures to determine the impact of such verification on aviation security and the Government Accountability Office has reported on its evaluation of the measures.

(e) TSA shall cooperate fully with the Government Accountability Office, and provide timely responses to the Government Accountability Office requests for documentation and information.

(f) The Government Accountability Office shall submit the report required under paragraph (a) of this section no later than March 28, 2005.

[6] Section 518 provides in pertinent part:

(a) None of the funds provided by this or previous appropriations Acts may be obligated for deployment or implementation, on other than a test basis, of the Secure

Flight program or any other follow on or successor passenger prescreening programs, until the Secretary of Homeland Security certifies, and the Government Accountability Office reports, to the Committees on Appropriations of the Senate and the House of Representatives, that all ten of the elements contained in paragraphs (1) through (10) of section 522(a) of Public Law 108–334 (118 Stat. 1319) have been successfully met.

(b) The report required by subsection (a) shall be submitted within 90 days after the certification required by such subsection is provided, and periodically thereafter, if necessary, until the Government Accountability Office confirms that all ten elements have been successfully met.

[7] This is a similar issue to that, discussed above, that reportedly plagued U.S. Senator Ted Kennedy.

The CHAIRMAN. Thank you very much.

Our next witness is Bill Connors, the Executive Director and Chief Executive Officer of the National Business Travel Association.

Mr. Connors?

STATEMENT OF BILL CONNORS, EXECUTIVE DIRECTOR AND CHIEF OPERATING OFFICER, NATIONAL BUSINESS TRAVEL ASSOCIATION

Mr. CONNORS. Mr. Chairman, pleasure to be here—Senator Inouye—thank you for inviting us.

Distinguished Committee Members, the National Business Travel Association's honored to be here today to participate in this discussion regarding the Registered Traveler Program and Secure Flight.

NBTA is the world's largest association of corporate travel buyers, corporate meeting planners, and travel purchasing professionals. A majority of the Fortune 500 companies in this country have travel managers within our organization. Our members direct millions and millions of business travelers each day. So, we're pleased to be here representing the interests of America's corporations, their travelers, and their ability to conduct commerce around the globe.

NBTA has been particularly focused on the issues of travel security and travel facilitation since 9/11. We're especially interested in the Registered Traveler Program, and look forward to its expansion. As a participant, myself, in the Registered Traveler pilot program here at Reagan Airport, I think the program offers business travelers two important improvements: productivity and predictability.

In recent NBTA surveys, we found that 92 percent of frequent business travelers have a desire to join an RT program, so there's clearly a demand for this concept.

NBTA has been encouraged by the recent vision set forth by Secretaries Rice and Chertoff regarding issues of security and travel facilitation. We've been further encouraged by a growing theme from our friends at DHS and TSA suggesting resources should be focused on the most serious potential risks to our Nation. The Registered Traveler Program is a good example of how smart risk management can both enhance the airport experience and allow for greater focus on finding potential bad guys. The RT Program will allow TSA to search a smaller haystack while moving people more efficiently through our airports.

NBTA has been a strong supporter of the RT Program, provided four basic requirements are met in any public or private administration of the program. Those four are, number one, that the program is strictly voluntary; number two, that the privacy of the participants is protected; number three, the program actually saves time for participants, while not slowing down nonparticipants; number four, the program is interoperable, secure, and overseen broadly by Federal authority.

We've heard a lot today about the Registered Traveler program, and while I'm aware there's great interest in this program, I am also aware that it's been very slow to materialize. Mr. Chairman, we could use your leadership on this particular issue. We would be happy to see you establish some specific program deadlines, and perhaps even recall this Committee three months from now to talk about progress on the Registered Traveler Program.

It is our hope that the RT program will be up and running in 2006 at scores of airports across this country, helping thousands of business travelers get back on the road to do the business of America.

Though we're largely here to talk about Registered Traveler, I would like to say a couple of things about Secure Flight. In regards to the Secure Flight program, we agree with many others here that airport screening procedures should use passenger data that is clean, clear, consolidated, and current. Pinging passenger names off multiple lists from multiple agencies yields multiple results.

The Secure Flight program must comply with the ten operational standards laid out by Congress and reported in the GAO report of March 2005. And we want to emphasize one of those standards in particular, which several others have emphasized here, as well. There must be a simple, secure passenger-redress system for removal from No-Fly lists. This must become a priority immediately in moving forward in any future program.

Finally, any changes in data-collection policies must consider costs to the corporations, the agencies, and the airlines who are asked to collect that data. That last point implies that involving private-sector in all of these discussions about passenger screening would help facilitate the program. In that regard, we again applaud the shared vision statement from Secretaries Chertoff and Rice calling for a private-sector advisory board to offer input on programs like the very two that we're talking about today.

The National Business Travel Association stands ready to support and serve with DHS and State in standing up such a body.

Thank you very much for the opportunity to be here.

[The prepared statement of Mr. Connors follows:]

PREPARED STATEMENT OF BILL CONNORS, EXECUTIVE DIRECTOR AND CHIEF OPERATING OFFICER, NATIONAL BUSINESS TRAVEL ASSOCIATION

Thank you Mr. Chairman, Senator Inouye and Members of the Committee. I am Bill Connors, Executive Director and COO of the National Business Travel Association (NBTA). On behalf of our members, I appreciate the opportunity to participate in today's hearing regarding TSA's passenger prescreening programs—specifically Secure Flight and Registered Traveler.

The National Business Travel Association is the authoritative voice of the business travel community, representing more than 2,700 corporate travel managers and travel service providers who collectively manage and direct more than $170 bil-

lion of expenditures, primarily for Fortune 1000 companies. Our members represent a broad cross-section of corporate America including millions of business travelers.

I want to first express the collective appreciation of the business travel community for your commitment to addressing the important issues of the Registered Traveler and Secure Flight programs and for including the perspective of the frequent business traveler in today's hearing. Our members share a common bond with many of the Members of this Committee in that travel is an occupational necessity.

Each day, thousands of business travelers arrive at airports across the Nation, ready to traverse the security checkpoints. Theirs is a perspective which differs significantly from other stakeholders in this process. Our Nation's most frequent travelers have a unique view of the effectiveness and the deficiencies of our current security regime, and it is vitally important that this perspective be considered in the debate over new security programs.

Business travelers over the past four years have experienced significant constraints given the cascading security requirements set forth by the Congress and implemented by the Department of Homeland Security. Business travelers are among the most experienced visitors at our airports and certainly understand and appreciate the necessity for these security measures to ensure national security and the continued viability of commercial aviation.

NBTA supports the goals of the prescreening and physical screening regimes put in place in response to the 9/11 attacks. In the aftermath of the terrorist attacks, business travelers were among the first passengers in the sky, and are again traveling in record numbers, as aviation levels return and even surpassing record levels. Over the past four years, one universal theme has been iterated by the vast majority of these travelers—we can and must establish more efficient and effective security measures by soliciting the cooperation of frequent travelers and utilizing available technologies to accomplish a less onerous and more effective level of safety and security.

Registered Traveler

The announcement by the Transportation Security Administration (TSA) regarding the national Registered Traveler plan was a welcome development for business travelers. RT pilot programs, such as the one undertaken at the Orlando International Airport, demonstrate that frequent travelers will embrace an opt-in system which provides a level of expediency and predictability to the screening process.

The RT initiative is a concept endorsed by the 9/11 Commission and Members of Congress as a way to enable security personnel to dedicate resources to more targeted risks. This concept is rooted in the belief that strong, effective travel security lessens unnecessary burdens on travelers. Registered Traveler is a demonstrable example that utilization of current technologies has the potential to provide the more than six million frequent business travelers with a more rapid, yet still secure screening process.

Affording passengers the opportunity to opt-in to the RT program provides a measure of predictability and reliability that corporate America has long sought. As companies seek to squeeze greater productivity gains out of their workforce, the ability of traveling employees to navigate through a web of security checkpoints in an efficient and reliable manner is critical in reducing time spent in the airport and increasing time spent conducting business.

Wait times at security checkpoints are anything but constant and current protocols dictate that passengers must arrive even earlier to ensure they are processed through security. Further, passengers traveling to different airports throughout the country have no ability to gauge wait times at each respective airport. While TSA has made measurable progress over the past year in addressing this issue, RT provides the promise that frequent business travelers will realize an increased level of measurability with respect to checkpoint wait times.

Much of the anecdotal evidence received from NBTA members participating in the Orlando International Airport pilot project indicates that RT participants indeed realized significantly reduced wait times. This was true even though the Orlando participants received the same security scrutiny (such as removal of shoes and coats) as did non-Registered Traveler participants. However, participants did benefit from access to a segregated security screening line. We fully expect that business travelers will derive even greater benefits when the full program is implemented and a complete slate of additional benefits is available to participants.

The success of the Orlando pilot project holds much promise for the potential of a national RT program, yet to ensure the fundamental success of the program, TSA must continue to address certain fundamental issues. TSA must continue to provide assurances that privacy concerns will be addressed in the implementation of the national Registered Traveler program. In a joint survey conducted by NBTA and the

Travel Industry of America, 92 percent of business travelers indicated a desire to participate in this program, and we expect that number to increase as the process becomes more transparent and TSA continues to offer assurances that passenger information privacy will be a primary tenet of the RT program. TSA's Registered Traveler archetype of a market-driven, private sector model must have informational safeguards governing the provision of personal information to third parties.

TSA has indicated that a core security assessment will be a requirement for each applicant seeking participation in the RT program, but more in-depth background checks using commercially available data may be undertaken by the private program providers. The trade-off for increased security scrutiny, as iterated by TSA, will be "a variety of enhanced or time-saving participant benefits at passenger screening checkpoints." As an opt-in system, RT applicants will have the final say in the information they seek to provide above and beyond the required TSA baseline information. Additionally, these enhanced security benefits could be derived through the deployment of additional security technology at RT checkpoints, such as Trace Detection equipment.

NBTA has joined many other stakeholders in this process in calling for a system of mandatory interoperability. Enrollees must be able to reap the benefits of participation at all airports engaging in the RT program. Corporate travel managers must be assured that private companies offering Registered Traveler cards will indeed work to develop a network where participants have universal access to RT privileges, regardless of the company providing the card. Additionally, interoperability will increase competition among companies offering RT cards, and as a consequence consumers will likely receive increased benefits at competitive costs. Stakeholder groups under the umbrella of the Voluntary Credentialing Industry Coalition (VCIC) have already initiated efforts to establish interoperability standards. These efforts signal a willingness on the part of industry to cooperatively engage with TSA in crafting a system that is viable and attractive to the business community.

Registered Traveler is a unique concept in the current security environment because it constitutes the first program dedicated exclusively to both traveler facilitation and focusing limited security resources in a threat based model. Significant progress has been made in outlining the RT program, and it will take the cooperative involvement of the aviation industry, government officials and travelers to ensure the system can continue to provide visceral benefits to participants.

Secure Flight

NBTA supports the steps taken by Congress to ensure the viability of Secure Flight before it becomes operational. As we all know, the current system draws too many people into secondary screening. Many frequent travelers have witnessed grandparents, children, and even Members of Congress unnecessarily selected for secondary screening. Not only is this process frustrating to the traveler, but it draws important resources away from the screening process. The process reflects the need to move forward in crafting a more pensive, comprehensive, threat-based model of security screening.

As TSA moves closer to launching Secure Flight, we urge careful consideration of several critical issues outlined in the March 2005 General Accountability Office (GAO) report to Congress. GAO described the progress that TSA has made in addressing the ten critical elements outlined by Congress, but GAO also appropriately recognized that additional progress is necessary leading up to the implementation of Secure Flight. Specifically issues of passenger redress as well as privacy concerns must be fully addressed in advance of the roll-out of this program.

It is difficult to discuss Secure Flight or passenger pre-screening issues without addressing the issue of passenger redress. Numerous business travelers have been ensnared on TSA's No Fly List or Selectee List, with little knowledge of how to navigate through the recourse process. These travelers then find out that they must complete the Passenger Identity Verification Form, mail the form to TSA, and wait for a finding. This antiquated system is time consuming and inefficient.

While the high profile cases of mistaken identity might provide amusing headlines, the hundreds of cases of mistaken identity involving less famous business travelers are just as serious. A recent survey conducted by NBTA found that over one-fourth of our member companies have over 5,000 business travelers per year. The frequency of business travel offers many chances for a case of mistaken identity and the disruptions that come with it. Many of our member companies struggle daily with watch lists issues that eventually are resolved, but the length of the process and the interim time spent waiting for resolution is costly to American businesses. An expedited process utilizing current technologies is not only possible, it's necessary.

Recently, Homeland Security Secretary Chertoff and Secretary of State Rice announced the Secure Borders and Open Doors initiative which included a proposal for "one stop" redress for travelers ensnared on the watch lists. This initiative promises a government-wide traveler screening redress process to resolve questions if travelers are incorrectly selected for prescreening. This is an extremely positive development, and NBTA fully supports the effort undertaken by both the Department of State and Department of Homeland Security to develop a system that utilizes current technologies to expedite passenger redress. As this system is being developed, TSA has indicated that it will continue to utilize its current Office of Redress to handle any watch list issues.

One of the fundamental problems of the current system is that most business travelers and their corporate travel managers are not aware of the procedures for redress. Even those travelers who are aware of their redress options find the current system exceedingly difficult to maneuver through. Many passengers have reported continued problems with repeated additional screening even after they have undergone all redress procedures and have been cleared by TSA. We urge that throughout the life of the current system and in advance of the implementation of the new passenger redress system, TSA undertake efforts to educate the traveling population on the steps passengers can take to resolve the questions of selection for additional screening.

While the problems with passenger redress may appear to be an individual problem, it has a definitive and collective impact on corporate travel planning. Similarly, seemingly insignificant changes to informational requirements have had significant financial impacts on several corporations. Secure Flight will require passengers to provide additional personal information in advance of travel. While this may seem innocuous to individuals required to provide the information, it poses some concerns for corporate travel.

Seventy percent of corporate travel managers currently utilize corporate online booking tools to capture the information necessary to book travel for their corporate travelers. That number is expected to grow to 90 percent or more within two years. And while there is no institutional resistance to making these appropriate changes to accommodate passenger prescreening, changes in the fields of information required by TSA would impose a significant cost on companies and businesses utilizing online booking tools, as they would have to revamp the software to capture and send newly required data.

Additionally, it is possible that information required by Secure Flight could force companies to undertake the cost of revamping internal privacy polices, as many companies currently prohibit providing employee personal information, such as social security numbers and date of birth, to third parties. NBTA encourages TSA to work closely with the private sector to ensure that Secure Flight can work with current and future systems used for booking travel. Corporate travel managers have made several changes to travel booking software over the last four years, and will continue to work to ensure corporate compliance with new security regulations. Yet, Federal officials must understand that small changes in informational requirements impose significant costs on corporate travel. From proposed CDC avian flu regulations seeking additional passenger information to Secure Flight informational requirements, costs on business could be significantly reduced if Federal agencies would work in concert to determine what type and format of information will be required and impose those requirements at one time.

The Secure Borders and Open Doors program may provide a framework for meeting that goal. Among the initiatives outlined in the Department of Homeland Security and the Department of State announcement, was developing an advisory board that would help determine best practices related to travel policies. NBTA supports this concept as we believe that this forum provides an opportunity to present unique private sector views to Federal officials in advance of significant rulemaking processes.

Ultimately Secure Flight will allow the U.S. government to focus more on the real threats and less on the millions of frequent travelers who are going about the Nation's business. However, there is a need for a clear and stable regulatory framework to guarantee free movement of personal and corporate data while maintaining privacy, confidentiality and security. More importantly, this framework will help to ensure consumer and corporate confidence in the exchange of information through the security screening process.

Mr. Chairman, I appreciate the opportunity to testify today, and thank you and the Committee for your leadership in recognizing the critical impact of these issues on business travel.

The CHAIRMAN. Thank you very much for that comment.

Well, Mr. May, I'm back where I started before. This is not the subject of this hearing, but the baggage still bothers me. And I know that you've got layers of security measures that you have to deal with. And the question I asked the other day was, Why isn't that little box that the bag has to fit in to go under the seat right there beside the screeners? I was told by people, when I objected to someone walking in front of me that had two suitcases larger than mine, and on the top of the little handle was a briefcase larger than my suitcase, and it had, obviously, a lot of computer stuff in it. Neither one of them would fit, hardly, in the overhead, let alone under the seat.

Now, doesn't the whole problem of these programs we're discussing here—aren't they affected by the time with which it takes to take all that baggage onboard an airplane?

Mr. MAY. Mr. Chairman, the good news is that I've had a series of conversations with some of our most senior executives since you and I spoke, night before last, on this subject. And, of course, it was a repeat of a conversation we had at another hearing in this room, a month or so ago. And I think the good news is that we share many of your concerns. The carriers are distinctly worried that people bringing on more bags than are allowed, bringing oversized bags, heavier bags, et cetera, is slowing down the process, it's having a real impact on productivity. And so, I'm here to tell you today that we are committed to pull the industry together to see if we can't come up with some very real solutions.

As you've identified, there was a time when those size-wise so-called requirements were put on the TSA screening equipment, so that if it didn't fit through that, size-wise, you had to go check it before you even went through security. And I think that and a number of other ideas need to be explored as to how we go forward. And I'll commit to you today that we're going to engage the industry in this right away.

The CHAIRMAN. Well, thank you for that.

Do you believe that this extra layer now in Secure Flight is necessary for security?

Mr. MAY. Senator, I think—quite frankly, I shudder to think of the hundreds of millions of dollars that have been spent on the bigger subject of passenger prescreening. And it's, quite frankly, been wasted money, because we don't have a program today. I think we absolutely have to have a program that is simple, straightforward, that matches passenger identification against appropriate watch lists, No-Fly lists, et cetera. There probably is not a bigger priority for us, and we're the ones, ultimately, that are paying for this. We care more about moving people through the process faster and efficiently than probably anybody else in the business. And so, I think that's where the focus needs to be. I don't think the focus needs to be, quite frankly, as popular as it may be, on Registered Traveler.

Mr. Hawley, my good friend, used the word "market-based," and I sort of cringe a little bit every time I hear that word, "market-based," when it applies to aviation, because it generally is translated into "airlines pay." And I know that TSA—I looked at their budget the other day—plans on making about $30 million, in this next cycle, on RT. I know that my good friend, Mr. Barclay, has a congressionally mandated monopoly on being the entity that

checks all this. That was put in the appropriations bill last year. I know that a number of other people are planning to make a profit off of Registered Traveler. And I don't—I'm a great free-enterprise person—I think that's all wonderful, but what I don't want to see is the airlines ending up paying for yet another failed program that doesn't work for everybody. And I'd like to see, instead, the focus placed on reducing those seven Government programs down to one, those 34 or more data requirements that we're being hit with, here and in countries all over the world, simplified to a simple template so that we have security that works here, security that works in London or wherever the case might be. And that's where the focus of this Committee ought to be.

The CHAIRMAN. I think we should take 5 minutes on each witness in this panel.

Senator Inouye?

Senator INOUYE. Needless to say, Alaska and Hawaii have unique problems. Interstate travel/intrastate travel require air travel. In fact, in our case, it's about 95 percent of the travel for the people of my state. And so, this is very important to me.

What sort of coordination do you have with TSA? Do they confer with you, or do you regularly meet?

Mr. MAY. Senator——

Senator INOUYE. I gather, from these discussions, that we have separate entities trying to undo each other.

Mr. MAY. Right. I think the fair answer to that question is that, historically, the door at TSA has always been open, the ears haven't necessarily followed. So, now we have an administrator that I think is doing a bang-up job. Very difficult circumstances. It's probably one of the tougher jobs in town. And I think Kip Hawley is really making some progress.

I'm pleased with the fact they're finally listening to complaints that we first registered with them back in 2002 and 2003 as to the multiplicity of these different passenger prescreening programs, the complaints that they've gotten on watch lists. But, as some of the other witnesses have said, they've got a mountain of problems in front of them trying to get all these programs worked out, getting a redress system put in place that's really effective, making sure you've got a watch list that's accurate, and a No-Fly list that's accurate. It's not an easy job. And I think we, and you, need to help them focus on that and on expediting everybody through the checkpoints with better technology, putting part-time workers on during peak times, finding ways to expedite pilots and crews, who are already certified, et cetera, so that we can really put the focus on where it's needed.

They're doing a better job. I think this TSA is the best I've seen in the time I've been in this industry. But they still have a ways to go.

Senator INOUYE. This question should have been asked of Mr. Hawley, but, as a matter of instinct now, I'm at the airport 2 hours ahead. And I do travel much, and over long distances. And I go through the metal detector, like all of you. I find that, over half the time, I'm given the special treatment, zip-zap all over the place. And here I am taking off my wristwatch, shoes, everything else, and coins. Do they adjust the metal detector?

Mr. MAY. Senator, it—you've asked me for my impression, and I think the answer to that is, yes, they do make some adjustments. Sometimes it seems that, when I go through—and maybe I've forgotten something that's in my pocket, and it doesn't set it off; other times, when I think I've really cleaned myself out, I set it off. So, I'm not sure but what there isn't a different adjustment available to them along the way.

I will tell you this. And it's sort of off the subject. This Committee passed legislation telling TSA that we wanted to ban lighters in baggage. We talked about the scissors, a little bit earlier. I'm advised that fully two-thirds of the bags that go to secondary search, that slow up the process for everybody, are as a result of those lighters. And I would suggest that, if this Committee does anything, it give very careful consideration to get rid of that ban, along with the scissors and some of the other things, because I think it will expedite the process for everybody immeasurably. And I'm not convinced that having a BIC lighter in your briefcase is a significant security threat.

Senator INOUYE. Do you pass on all of the costs incurred through Government activity to the passengers?

Mr. MAY. No, sir. I wish we could. We don't have the pricing power that we would like to have. And that's why that $4 to $5 billion a year that we're paying to DHS and TSA hits us so hard. I mean, I look at an agency that has remained relatively flat in their budgeting since their inception—it's about 4.5, 4.6 billion—and I see our fees have gone from that billion-250/260 range up to 4 billion without, by the way, any additional congressional or Administration mandates. That's just the growth of—based on the fact it's a ticket tax, and we've got more fees going in, with the minor—there have been administrative increases in the Customs fee and the Agriculture fee, for example. So, it's mission creep—in this case, it's tax creep—that hits us.

Senator INOUYE. Senator Nelson asked a very interesting question, that, at several airports, you have two lines, first class and——

Mr. MAY. Right.

Senator INOUYE.—economy. Do you have any good rationale or justification for that?

Mr. MAY. I think—I think the——

Senator INOUYE. I can see where, first class——

Mr. MAY. Sure.

Senator INOUYE.—you could have a bigger seat and all of that. But on the security?

Mr. MAY. Senator, there are expedited lines available in a number of different—principally hub airports—all over the country, where individual carriers permit their frequent flyers and first-class passengers, to move up in what generally is a partially separated line, because it then gets merged, because everybody goes through the same level of security, no matter what. They don't have special security treatment. And to the extent that frequent flyers and others have a benefit, I think that's perfectly appropriate.

What I think ought to happen, though, is, once those two lines merge, that we have an overall security process that is even faster

and better than the one we have today. And that's where I'd like to see us focus. Rather than reducing some of those security requirements to benefit a very few people, let's have it available for everybody.

Senator INOUYE. None of us here are technicians. It would help very much if all of you can get together and tell us how this consolidation of programs can be carried out.

Mr. MAY. We have a series of suggestions in my written testimony, Senator—I encourage you and your staff to look at those—as to how we can bring some of these programs together.

Senator INOUYE. I'm very concerned about identity theft and privacy and all those matters, as you know.

Thank you very much, Mr. Chairman.

The CHAIRMAN. Senator Burns?

Senator BURNS. I have, after listening to all the testimony and then reading everything that's in the paper—and, by the way, Senator Inouye, I could be riding first class, but I stay over there in the economy class, because I'm afraid somebody will hit me in the head with a bag when I go walking down through there. I don't want to cause a scene or anything.

Senator INOUYE. A man of the people.

Senator BURNS. That's right, a man of the people is exactly right.

I just have one question. Do you still support the Registered Traveler and the Secure Flight programs? Are you still supportive of those programs, even though we're struggling to get them in place in a proper way?

Mr. MAY. Senator Burns, from the ATA perspective, we absolutely support the concept of Secure Flight, or whatever name you want to give to passenger prescreening. It's the concept that we support. We don't support, at this time, Registered Traveler. We think it takes the focus away from where we really ought to have it.

Senator BURNS. Mr. Barclay?

Mr. BARCLAY. Senator, airports strongly support both programs.

Senator BURNS. Mr. Sparapani?

Mr. SPARAPANI. That's excellent, sir, actually. Thank you, Senator.

As I said in my statement, we think that both programs ought to be scrapped, and, instead, what Congress should do is insist that we retain this idea of focusing on a watch list that's vastly pared down to really known threats to aviation security. That's where we need to put our energies into. Those are the people we need to stop. And I don't think that's inconsistent with what Mr. May just said to you. In fact, I think if you just whittled that list down, and then prescreen against that smaller list, you'll have far fewer of your constituents who are stopped or put on these lists and can't get off of them. So, there's some consistency here on that part.

Senator BURNS. How do we find these bad people?

Mr. SPARAPANI. We're going to have to do some work. And our Government's going to have to spend some time doing it. I'll leave that to the intelligence experts. But I will point out, for these two programs, they're premised on a faulty premise, which is that—one that we reject, and I think most intelligence experts would reject—that terrorists are going to show up, buy a ticket—attempt to buy

a ticket, and attempt to show up under their own name or documents. Once we know who they are, they're not going to do that. That's a pre–9/11 mentality. Identity theft is just simply too easy, Senator.

Senator BURNS. Mr. Connors?

Mr. CONNORS. Senator Burns, we agree with our colleagues at ATA in supporting Secure Flight, particularly what Mr. May has said about having a uniform passenger information-collection policy.

We differ a little bit on our views of Registered Traveler. We certainly encourage the expansion of the Registered Traveler program so that all citizens who are interested could go through the same sorts of lines that Mr. May just described for first-class passengers.

Senator BURNS. Well, I've looked at this thing, and they keep struggling over there, and I take to heart what Mr. Sparapani said. How long do we fiddle around with this thing before we finally get something that will work?

I support the Secure Flight program. And, even with the Registered Traveler, I'd be willing to buy a card, I think, you know. But, nonetheless, we've got to, some way or other, draw some conclusions and either take what we've got and go with it or dive completely out of it. It sounds like, to me, we're making work. That's what I'm saying. And we're just throwing good money after bad. And money that we don't have, by the way.

And so, those are the questions I had. I'm opposed to increasing the tax, I will tell you that right now. I'll——

Mr. MAY. Thank you, sir.

Senator BURNS.—go on record. Right now, you look down that ticket, and they're going to have to make a bigger ticket. Not for a guy that's got a bigger name, or the seat, but how many taxes you're going to list on that darn thing. And so, it's from that standpoint that I'm pretty up-front about these fees.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator BURNS. And thank you for your testimony. I appreciate it. We've gleaned a lot of stuff from it.

The CHAIRMAN. Thank you.

Chip, when we look at this program, the new Registered Traveler program, it appears as if it was merged with an eye-scan concept or something, that it would give us a chance to deal with people who are really frequent flyers. Now, when you look at that program—have you looked at it from the point of view of fraud? Can it stand up alone? Can we depend on those cards? Do we have to have the eye scan to go along with them?

Mr. BARCLAY. The—well, let me go back and say that the big distinction—and I think Senator Burns' comments about the two different programs points it out—Secure Flight, it's a much harder program, because it is looking for terrorists. Registered Traveler is about identifying people, at least at first, that we know are not threats to the system. That's something that we can do. We can figure out who are people that don't threaten the system. We can avoid the problems that have been raised about identity theft and other problems by making sure biometrics are part of the system. And that can be eye scans. Some people that may be handicapped

and wouldn't have the ten fingerprint can use eye scans. You can use the fingerprints. So, you make sure, each time that person you identified as not being a threat to the system goes through, you know that's the person that you've got there, because of the matching of the biometrics.

It's very similar to what we're trying to do at airports with the access to secure areas, putting biometrics on many of the doors to make sure that, once we vet a person and know they're not a risk to the system, we know we've got that person every time they go through a door.

We need to do the same thing with frequent flyers in the system, because, as everyone here knows, if you are someone who uses the system a lot, you're putting aside a lot of extra time in case—not because there are often delays or long lines winding through the terminals, but there are, occasionally, so you put aside that extra hour every time you fly. The productivity loss to people and the economy is enormous. And we have these fairly small number of people who represent a great percentage of the passengers that want to be treated like employees at the airports are treated now.

If I can make a point, one thing that I think a lot of people don't realize is that every day in this country we let hundreds of people on airplanes with loaded guns because we've done background checks on them, and we trust them not to be dangers to the system. We could certainly let people, after doing the same kind of background checks on them, not take off their shoes and not take out their laptop, and vet them through the system more quickly so we can direct our security assets to the highest risks. That's what Registered Traveler is really about. It's saying, we've got limited security resources, let's use them on the highest risks, because we've got a lot of people who volunteer information on themselves and pay for the program to be able to eliminate them from the risk pool.

The CHAIRMAN. Well, I thank you for that. I do think there are a great many of those frequent-flyer people who will go to the Registered Traveler Program. Their time is money. I mean, they are compensated by the hour. This system, currently, really is denying them the use of the valuable time, daytime, that they have to use in pursuing their livelihood. I think it's a good program.

Mr. Sparapani, I am a little disturbed about your testimony. And you want us to revoke the authorization for both Secure Flight and Registered Traveler and set up a process to deal with known terrorists.

Mr. SPARAPANI. I do. That's——

The CHAIRMAN. Have you——

Mr. SPARAPANI.—that's correct, Senator.

The CHAIRMAN.—have you got a list of known terrorists?

Mr. SPARAPANI. I'm sorry?

The CHAIRMAN. Have you got a list of known terrorists?

Mr. SPARAPANI. No. But the——

The CHAIRMAN. Do you think——

Mr. SPARAPANI.—the government——

The CHAIRMAN.—we have a list of known terrorists?

Mr. SPARAPANI. I think the Terrorist Screening Center does. And that's the public statement from the FBI.

The CHAIRMAN. Well, I'm——

Mr. SPARAPANI. And——

The CHAIRMAN.—I'm not so sure. Do you support the President's program right now that's under attack, in terms of intercepting and tracking the people called within this country from outside of the country? You support that?

Mr. SPARAPANI. Well, I don't want to equate the two programs, Senator.

The CHAIRMAN. Well, I'm asking you if you support it. You oppose it, don't you?

Mr. SPARAPANI. I—we do oppose the unconstitutional application——

The CHAIRMAN. Well, then what's——

Mr. SPARAPANI.—of that program.

The CHAIRMAN. What do you support to determine who is a terrorist?

Mr. SPARAPANI. When we have good intelligence that has identified a threat to aviation, we believe there should be a list of those people. This is just commonsense safety and security. That's the list that I want the Government to use to screen for aviation security. And I think if we do that, Senator, we're going to have vastly improved security without all the civil-liberties deprivations that might arise from a bloated list. We can't simply have every Senator Kennedy—everyone who has a name like Senator Kennedy being stopped every time, because there's an E. Kennedy on a list. You mentioned your wife's situation——

The CHAIRMAN. Well, Kennedy was embarrassed, but I don't think he was really hurt. And I don't think any of us are hurt by trying to have the system check us to make sure we are safe to get on the plane with other people who are traveling. You seem to believe, though, we should somehow or other dream up a list of known terrorists, and only they should be subject to screening.

Mr. SPARAPANI. I think we need to put our focused resources onto those people who pose the threat. And if we do so, Senator, I really believe that we're going to have vastly improved security. We want to—we really want to focus on those people who have the capability of threatening airline security, and we want to keep that list close. Right now, some of that list goes to the airlines every day, but not all of it. So, we're not currently——

The CHAIRMAN. But—wait a minute——

Mr. SPARAPANI.—vetting against——

The CHAIRMAN. But that's not your statement. You say you do not oppose the Federal Government keeping and maintaining a list of terrorists known to pose a threat to aviation security.

Mr. SPARAPANI. That's correct.

The CHAIRMAN. If a person is known to be a terrorist that has other targets in mind, you would let them on the airplane, right?

Mr. SPARAPANI. No. Senator, if somebody's been violent, I would consider that somebody who is a threat to aviation security.

The CHAIRMAN. Well, how do you define a person who's a threat to aviation security as a terrorist, as opposed to other terrorists?

Mr. SPARAPANI. Again, if somebody's violent, Senator, and has a propensity, and the Government has good intelligence based on that, we don't oppose having a list of those people.

The CHAIRMAN. Respectfully, we don't have a list of people who are known to be a threat to aviation security. We are looking for terrorists——

Mr. SPARAPANI. Well, if that's true, Senator——

The CHAIRMAN.—generically.

Mr. SPARAPANI.—if that's true, Senator, then the No-Fly list itself is——

The CHAIRMAN. All right.

Mr. SPARAPANI.—is faulty.

The CHAIRMAN. Well, I—you make some points in your testimony that appeal to some of us, in terms of trying to find some way to get to the point where we really have a system that works, but then you come down and say, "But it should only apply to people who are a threat to security." I just cannot buy that. And I think that you destroy the value of your comments by telling us we should have a list of terrorists who are a threat to aviation security. I assume we'd have a list of terrorists that pose a threat to Federal buildings. This is getting down to the point where I just don't think we can find a way to predict terrorist acts.

Mr. SPARAPANI. And, Senator, we have an extra additional recommendation, which I think would resolve the concern that you're raising. We suggest that the money saved should be spent on those high-quality, narrowly tailored screening technologies, like this new puffer machine; if done right, that will prevent weapons and explosives from getting on planes. And if you do those two things, I think you're really going to demonstrably improve airline passenger safety and security. And I think that's what we all want.

Senator BURNS. Would the Senator yield on that point?

The CHAIRMAN. I'd be happy to yield.

Senator BURNS. Explosives being carried on the airplane is not the danger. They're not blowing up the airplanes; they're running them into things. I think, basically, that's not the priority. And then, how do you—if we don't, under a suspect, have the right to surveil, I don't see how we find these people. Some way or other, it seems to me that we have forfeited a little bit of our right to privacy whenever terrorists decided to operate like they're operating now. And to seek those people out who are the high-risk people, that's really the travelers program. Yes, that deals with the majority of us; we're the known. But whenever we get over to standing—oh, about the clandestine and the unknown, I'm going to leave that to the clandestine and covert people to collect that information.

But to take a rigid line saying the President is—I'm not going to argue the legal end of it, but I will tell you, if I was sitting in that school room, and my aide comes in there and tells me I've got two buildings down, the Pentagon's been hit, and there's a plane down in Pennsylvania, and I've got to make a decision, there's not very many of us that have occupied that seat, and I want all the information I can get before I jump, but I don't have a lot of time to jump. And we're all sworn to protect this country against all enemies, foreign and domestic. And I think we're venturing into an area here where we all sacrificed a little bit when what happened on—at 9/11. We all sacrificed.

Thank you very much, Mr. Chairman.

The CHAIRMAN. Mr. Sparapani, has your organization taken a position on the increase in fees for airline passengers that was discussed here?

Mr. SPARAPANI. Not directly, Senator. I wouldn't want to speak whether it's good from a free-enterprise perspective or not for these fees. But we all want the flying public to be safer. We're trying to help. We want to work with you and this Committee, and the TSA, to make the flying public safer. And that's the goal that we have and we cherish, as well.

The CHAIRMAN. Thank you.

Mr. Connors, do you depend on a poll of your members to present the statement you've presented here today?

Mr. CONNORS. Presented—I'm sorry?

The CHAIRMAN. Did you rely on a poll of your members, or some way to contact your members, for the statement that you are representing the whole National Business Travel Association. I take it these are operators of travel bureaus and things like that, right?

Mr. CONNORS. No, actually our members are people within big corporations across the country who direct, manage, purchase, travel on behalf of all——

The CHAIRMAN. I see.

Mr. CONNORS.—of those corporate travelers.

The CHAIRMAN. Well, thank you——

Mr. CONNORS. So, they're not agencies; they're within corporate——

The CHAIRMAN. How did you——

Mr. CONNORS. But, to answer your question, we did make a reference to a survey that we did with our friends at TIA, where we surveyed frequent business travelers. And 92 percent of those wanted in on a concept, whatever that concept may look like in the end, called Registered Traveler.

And I'd go a step further and—whether we have research or not, you've got an experiment down in Orlando that shows that there's a tremendous demand for this. You've got only one airport, no interoperability, yet you've got 15,000 people down there who are willing to pay 80 bucks, give up all sorts of background information, and go through background checks. This obviously is going to have tremendous demand once you get more than one airport into the system.

The CHAIRMAN. Did you discuss a limit on the cost of that card?

Mr. CONNORS. We haven't discussed that, and I think the marketplace would bear that out.

The CHAIRMAN. Do you have a list of what registered travelers would be willing to disclose to get a card?

Mr. CONNORS. Well, that's an interesting question. And we're looking to TSA, to explain what they are going to ask for and what they will get in return. There are two models that are being discussed, as far as Registered Traveler goes. There is the trust model, which is the one that you're talking about, where we ask for more and more background information, and, based on that, we'll give you the OK to be in the program. And there is the technology model that says if we invest in certain technologies, we won't need as much information, whether it's foot-screening equipment, things like that to get people through without taking their

shoes off and all that kind of thing. We're interested in pursuing both models but, again, we're just waiting for the details about what you need to provide for what you get.

But you know, and I know, that there's a spectrum of people out there that won't be interested in this program at all. They don't want to give up background information. That's fine. It's a voluntary program. Then there are people on this end of the spectrum—and I throw myself in this—who would probably give you blood, hair samples, DNA, whatever it is, to get through that airport faster.

And I think the experiment in Orlando shows that there's a tremendous demand for this, even though the benefits are pretty minimal at this point. It's one airport. And you can talk to the folks who are running that program. There are people buying cards for the Orlando Airport experiment who don't live in Orlando. They're just buying it on the back-end trip, because they do business there.

So, we think there's tremendous demand. And you made the point that we make all the time about this particular program, and that is, time is money. I represent America's corporate travelers, and time is, indeed, money. I was a Registered Traveler here at Reagan Airport, and that program is no longer in use. When I go to the airport now I have a whole different time that I leave for the airport now. When I used to be in that program, I used to leave an hour before, and now I have to leave two 2 hours before. That's an hour, times every single trip that I take. Time is money.

The CHAIRMAN. Have you participated with TSA in the discussions of the details of the Registered Traveler program?

Mr. CONNORS. We have, and we have been pleased that at least they've said, "Yes, we're going to the next step." Again, we would like to see more details about what they're going to ask for, in terms of data on folks, and what they're going to offer, in terms of benefits.

The CHAIRMAN. I failed to discuss this with the prior panel, but I found out, in recent travel, that if you buy a one-way ticket to a certain destination—let's take California—I was going there, and then I drove from that destination to another place, and then I had a ticket, going on. I was treated differently than if I had had a ticket going from the first location. These segments are separated, and it brings about an additional delay. Do you think the Registered Traveler program can be managed to take out that delay so that a person having a series of tickets that are sort of looked at like they're one-way tickets would be treated the same way as someone who had a roundtrip ticket?

Mr. CONNORS. Right. Ideally, that's where we'd like to see the program go, that there is interoperability between airports. So, all I need is my biometric card, and I won't have that issue, whether it's at that airport or the one that I'm transferring to. So, that's why we're hoping for interoperability. Additionally we know that the companies that are running this have airports signed up already. They're just waiting for that green light from TSA.

The CHAIRMAN. Mr. May, I think as everyone realizes, this Committee has jurisdiction over the airline system, as well as the TSA system. But we are very worried about the cost of these layered systems to the commercial aviation system, passenger system, be-

cause they're already in trouble, with increased fuel costs and increased costs all over the system. Have you got any estimate of how much the industry itself has spent on security since 9/11? I mean, talk about what the companies have paid for CAPPS I, CAPPS II, Secure Flight, and now planning the registered system.

Mr. MAY. Senator, I don't have any hard-and-fast estimates in the aggregate since 9/11, but I think it's fair to say that we've gone from spending somewhere in the range of $2.5 to $3 billion a year in imputed costs as a result of those security measures that we are required to perform because TSA won't; i.e., that ticket-checker that you see when you stand in line is paid for by the airlines, not by TSA. When there is catering security, cargo security, it is paid for by the airlines, not by TSA. So, we've gone from roughly $3 billion a year at the outset, of what we were paying in a total of taxes, fees, and imputed costs, to now something well over $4 billion, and if the Administration's proposals were to be adopted on the ASIF fee and the segment tax, you'd add another billion-four or -five to that. So, if you multiply out—that out times the number of years, it's double-digit billions of dollars that this industry has paid for what we fundamentally believe is a function of national security.

The CHAIRMAN. Do you have any more questions, Senator?

Senator INOUYE. No, thank you.

The CHAIRMAN. Well, we thank you all for coming. We thank the first panel, too. I do believe Mr. Connors has a point and that is that we have an ongoing review of the system. So, I would like to assure you that sometime by the end of May, we will be asking for additional information to see what, if anything, we might have to do to suggest a change in law or to find a way to deal with the complications of this security system. The airline passengers are the only ones that are paying for their security today, and the airline companies are the only ones that are really paying totally for the security. And I think that the security system across all modes of transportation needs to have a review. We'll talk about that later, too.

But we do appreciate what you're doing. I think, Mr. Hawley, we're pleased with the way you're moving forward and trying to get this program really to the point where it has greater support from the public. All of us in Congress, I think, get as much comment about this subject, of the delays in air transportation and the impacts of the security program, than any other subject we deal with.

So, we hope to be back and have a—if not a formal hearing, at least a discussion with the participants sometime by late May to see what's happened and what, if anything, we can do to assure that this program will mature and get to the point where it has, really, the support it needs from the traveling public.

Well, we thank you very much.

Senator do you have anything further?

Thank you all very much.

[Whereupon, at 11:55 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

Thank you Mr. Chairman for holding this important hearing to review the Transportation Security Administration's Aviation Passenger Pre-Screening programs.

The TSA faces a challenge ensuring the safety of those who travel on our airlines while preventing the screening process from becoming overly burdensome. While I understand the dilemma of balancing security and civil rights, I support the TSA's attempts at determining potential risks prior to their boarding.

I am concerned about potential cuts to Transportation Security Officers at Portland International Airport (PDX) from 509 full-time equivalents to approximately 356 full-time equivalents. This reduction is one of the largest decreases among U.S. airports both in percentage and in absolute terms.

PDX is a critical transportation facility for both Oregon and Washington and plays a vital role in the Pacific Northwest's economy. Serving 13 million passengers annually, Portland International Airport handles more than a quarter million tons of air cargo and provides 31 carriers with more than 500 passenger flights daily. It impacts over 75,000 jobs in the Portland metropolitan area and generates $3.5 billion dollars annually for the region.

Passenger traffic at PDX is growing dramatically, not shrinking as the cuts in the screening force would suggest. The current screening force at PDX is already struggling to handle existing passenger loads. A cut of this magnitude would increase passenger wait time and lead to a reduction in security for planes leaving Portland. Additionally, these concerns are shared by the Port of Portland. which owns PDX.

I am concerned about the impact these cuts will have on the Portland International Airport's security screening process, the stress this will place on the screeners and the amount of time it will take for the airport's passengers to proceed through the security line.

Thank you for taking your time to come before this Committee. I look forward to your testimony.

PREPARED STATEMENT OF KEVIN P. MITCHELL, CHAIRMAN, BUSINESS TRAVEL COALITION

Mr. Chairman and Members of the Committee thank you for inviting the Business Travel Coalition (BTC) to submit testimony on this important subject, and for your interest in the views of the customer of the commercial air transportation system.

I. Background

In the weeks immediately following 9/11, BTC conducted meetings in every region of the country to identify barriers to the return of business travelers to the skies, rental cars, hotel rooms and restaurants. A major theme in those meetings was the need for some sort of pre-screening program for business travelers, referred to then as "trusted traveler." BTC has been advocating such a program since.

During the ensuing years, Congress, DOT, TSA, DHS and other industry participants' interest has waxed and waned. However, business travelers have never lost interest in the now-called Registered Traveler (RT) program. BTC surveys since 2001 and right up to January 2006 show a huge airport security screening problem and great business traveler frustration. Thankfully, Congress and TSA are now fully committed to RT program implementation, though misperceptions about the program and some marketplace confusion remain.

II. Problem Statement

"It is faster to clear El Al security than to get to the gate at a U.S. airport. It has taken me over 2 hours to reach the gate at Honolulu, San Diego, Rochester, Albany and DC in the past two months. Security is critical—but there MUST be a better way."

This is a representative quote from one of 644 business travelers who participated in a January 2006 BTC survey. During peak business travel times, security screening wait times can vary widely. This is a huge problem for business travelers, 64 percent of whom responded that without a RT program they believed that wait times at their home airports would likely get worse. With air passenger growth expected to be 3 percent to 5 percent over the coming years, and TSA's screening budget shrinking, these travelers' concerns appear well-founded.

In a June 2005 BTC survey of 651 business travelers, 37 percent indicated that long lines were their #1 concern. Some 38 percent indicated that inconsistency of

screening processes and the unpredictability of wait times among airports was #1. Some observers dismiss such concerns by referring to average wait times posted by TSA. As a success metric, average wait times obscure much higher peak travel wait times, which tend to disproportionately impact business travelers, for example, en route to early morning meetings. *This metric becomes more meaningful when the extra time that business travelers must pad their schedules with, due to screening time unpredictability, is added in*.

Unpredictability of wait times steals the business traveler's valuable time. Not knowing whether an airport security line will be 5 or 50 minutes long requires that business travelers arrive at an airport 90 minutes or more in advance, sometimes cutting short a productive meeting with a client or important work in the office. The enterprise-wide productivity of the corporations that fund business travel activities is negatively impacted, and by extension, so is the national economy.

Handicapped business travelers are especially impacted by current screening processes and have been given very little attention in this debate. Theirs is an airport security experience of extra time, inconvenience and stress. Consider these statements from business travelers writing to BTC:

> *"Give me a photo ID or take a picture of the stump of my missing right foot so I don't have to undress each time I travel using airports."*
>
> *"I'm handicapped missing my right foot. I wear special shoes. When I remove my shoes I can't walk, I can only hop. Why can't TSA give me a photo ID stating I'm handicapped so I'm not held up for additional screening?"*
>
> *"I have metal knees and activate the walk-thru detector. If I do not set it off, it is not working properly but I keep my mouth shut to avoid an airport lockdown. Thus, I know I will be subject to secondary screening and will have to take off my shoes."*

III. Market Demand

In an April 2002 BTC survey of 181 corporate travel managers, 69 percent of respondents indicated that they thought their travelers would support a "Trusted Traveler" program. In a follow-up June 2002 survey of 408 very frequent business travelers, 72 percent indicated they would support a "Registered Traveler" program to speed and improve the quality of airport security processes. Fast forwarding to a 2005 BTC survey, 77 percent of business travelers indicated they would "strongly support" or "support" a Registered Traveler program.

Of course, surveys do not always tell the whole story. It was not until July 2005 that the industry had a chance to see if true marketplace demand would materialize. The Orlando airport contracted with a RT service firm to provide services for $79.95 per member, per year. Over 14,000 travelers have enrolled to date. Feedback from members has been overwhelmingly positive. (Listen to RT member interview on BTC Radio at *http://btcblog.typepad.com/btcradio/*.)

Another important indicator of demand is that the majority of major North American airports are actively investigating the RT program responding to business traveler demand in their markets. Several have already made decisions to implement. Likewise, many North American airlines are keenly interested in the program.

IV. RT Program Benefits

A. RT Members

The major benefit of a RT program, from the perspective of the business traveler, is the high degree of certainty regarding an efficient processing through airport security. There are other benefits under consideration by TSA such as not having to remove shoes, laptops, or outer clothing. Such benefits will come after RT service providers implement enabling service lane technologies.

Notwithstanding the importance of the benefits above, RT members stand to benefit in other ways such as:

1) **Customer Service.** A RT program member at Orlando called the customer service "beyond excellent" and spoke of being "pampered" by the RT service provider's staff. This is important and valued by business travelers.

2) **Interoperability.** Today a business traveler flying out of a major hub likely has access to an airline's Elite security line, if they qualify. However, *at least* 50 percent of a business traveler's experience is at his non-home airport where there may or may not be an Elite line hosted by his preferred airline. Moreover, many business travelers originate out of mid-size airports where such Elite lines may not exist. TSA has rightly set a standard that mandates that a RT member can use his card, without additional cost, at any airport serviced by any RT service provider.

Interoperability is not a big technological challenge. (See Addendum: BTC Interoperability Statement).

3) **Boarding Passes.** The ability to go through security and secure a boarding pass on the air side would benefit business travelers and bring relief to kiosk stations during peak times.

4) **Smaller Land Side Crowds.** Avoiding large crowds on the relatively low-security land side of an airport is important as airport lobbies have been historically high profile, easy terrorist targets. Moving business travelers through security efficiently, and improving overall security system throughput, is prudent risk management. Corporate Risk Managers would value having traveling employees enter the more secure air side of an airport as quickly as possible.

5) **Safer Travel.** Since 9/11, the so-called security hassle has caused many business travelers to drive their cars in short-haul markets (under 500 miles). The fall-off has only partially rebounded. Southwest Airlines, for example, still reports a 20 percent decline in short haul for its Love Field operations. Driving a car is exceedingly more dangerous than traveling by airplane. More efficient security would help save lives on the highways, reduce congestion and help the environment.

6) **Handicapped Travel.** Greater respect, customer service and convenience await the thousands of handicap travelers who navigate North American airports.

B. Benefits: Traveling Public

1) **Faster Processing.** A properly functioning RT program, in the mold of the interstate electronic fast pass tolling, will improve the overall throughput for non-RT program travelers saving them time. For example, a dedicated RT lane, that represents 10 percent of the throughput capacity, could actually handle 15 percent or more of the passengers due to the prescreening and service configuration efficiencies. *Public security lines will not become longer*. Moreover, where physically feasible, RT vendors will likely pay for the construction and equipping of entirely new lanes.

2) Smaller Crowds. With business travelers bypassing land side kiosks for boarding passes and moving through security quickly, and overall faster security system throughput, the traveling public's experience and safety will improve.

C. Benefits: TSA

1) **Optimizing Limited Resources.** Air traffic is expanding, TSA's budget is shrinking. RT allows TSA to NOT focus on 100 percent of passengers as if they were all equal threats to the aviation system. RT will allow TSA to focus its limited resources of money, time, people and equipment on a smaller subset of the traveling public.

2) **Enhanced Security.** In joining a RT program, a traveler receives better service in return for being subjected to a higher level of information-based security, and physical security screening. An example would be a shoe scanner that is paid for by the RT provider and deployed to identify explosives. Such a device would be used so that a RT member would not have to remove his shoes. This technology is superior to X-ray machines currently used. *As such, the 10 percent to 15 percent of travelers who generate 40 percent to 50 percent of airports' traffic will actually receive greater security scrutiny making the overall system more secure.*

3) **Crowd Control.** As mentioned, TSA's mission would be supported if the large crowds that often build up on the land side were significantly reduced.

4) **Customer Service.** TSA will be implementing a randomizing of RT processes and benefits. This represents a best-in-class security approach in use throughout the world and is not mutually exclusive of the desire of business travelers wanting more certainty in the screening process. What business travelers want is the certainty of the amount of time they will need to budget for security, not the absolute predictability of process components. Add to this the enhanced customer service provided by the RT providers and TSA can be commended for improving the customer service result.

D. Benefits: Airlines

1) **Cost.** RT service providers and their customers will incur all the costs of establishing, marketing and operating the program. Moreover, some RT providers will likely be willing to revenue share with airlines in turn for their help in marketing the program to their frequent flyer bases.

2) **Additional Passenger Revenues.** The last 6 airline passengers who board typically make the difference between profit and loss on a given flight. A consistent, positive security experience will bring back many of those high-yield business trav-

elers who have abandoned airlines for automobiles, trains, limos, buses, fractional jets and other options, including not taking a trip.

3) **Customer Service.** The RT program will provide the opportunity for exceptional customer service for airlines' best customers.

E. Benefits: Airports

1) **Better Service.** Business travelers can comprise 10 percent to 20 percent of an airport's total customer base, but 40 percent to 50 percent of its traffic. Clearly it is every airport architect's and operator's mission to service these important customers well. RT is a strategic solution to this problem.

2) **Revenues.** Winning back business travelers who have defected to other modes of transportation or communications technology, e.g., video conferencing, is a priority for airports. It has a direct bearing on maintaining air services to many markets. Likewise, airports benefit from greater parking and concession revenue with increased numbers of business travelers.

3) **Crowd Control.** As previously mentioned, moving passengers from the less secure land side of an airport to the air side enhances the overall security environment. Additionally, the more time passengers have on the air side, the more they will spend in stores generating revenue for the airport.

V. Private Sector Rationale

The private sector's primary role will be to work with airport authorities to establish and market a RT program. TSA will set and oversee security standards. RT providers will be encouraged, through marketplace forces, to continually enhance the customer service experience in the RT lane. The competencies required for success include branding, consumer marketing, subscription-based services and strategic marketing alliances. These are not the usual competencies found in governments.

VI. Privacy

Business travelers have become sensitive to data privacy issues, particularly over the past few years. TSA and airlines have misused data, and commercial data aggregators have failed in their mission to protect consumers' information. Identity theft is on the rise. For RT to work system-wide it needs a critical mass of members, supported by low member costs, met service expectations and strict privacy protections.

The Orlando RT model, having generated 14,000 members to date, appears to have hit the mark with the RT service provider's data privacy commitments. TSA's proposal to use commercial databases as an exclusive way to provide additional RT program benefits is overreach in BTC's view, and could significantly dampen business traveler demand for the RT program.

VII. Equity

Some observers are of the view that the RT program asks a citizen to pay a fee to demonstrate that he or she is not a terrorist risk, and some find this offensive. However, no one is asking a citizen to do anything. The marketplace and capital providers are simply offering a service. Moreover, travelers are paying today, through TSA security fees, to demonstrate that they are not terrorist threats before they are allowed to board a plane. Importantly, all costs associated with the RT program will be borne by RT service providers and their customers, not taxpayers.

Mr. Chairman, BTC is very supportive of the RT program and appreciative of a renewed TSA commitment to reach out to the travel industry for input. We believe we are on the cusp of creating the best airport security protocol in the world.

Thank you for the opportunity to contribute.

ADDENDUM: BTC INTEROPERABILITY STATEMENT

Registered Traveler Interoperability

Business Travel Coalition, January 2006

The June 2005 launch of the Orlando Registered Traveler program marked the expansion of the Registered Traveler program to the private sector. The Transportation Security Administration (TSA) had incubated the program by testing technology and piloting the overall concept at five airports. With Orlando, it was turned over to the private sector for a rollout that would be self-supported. Orlando Registered Travelers have begun to receive their Clear Cards, from Verified Identity Pass Inc., the program service provider, and are utilizing a designated "fast lane" and line at Orlando airport.

As Registered Traveler (RT) programs expand, travelers will be able to use fast lanes at other airports across the country. Since TSA has mandated that private

sector RT programs be interoperable, Registered Travelers will benefit from the program network no matter what company provides their card.

Standards To Be Set

Since testing the technology in the pilots, TSA has aimed to make the programs interoperable so that members who enrolled at Los Angeles, for example, could use their cards at Dulles. Making the pilot programs interoperable has been more difficult than it will be to make future RT programs interoperable. That's because, in order to test different technologies, TSA purposely created five completely separate programs that used different hardware and software. That was the point: to test different technologies. This complication makes linking the pilot pro-grams, so that they are interoperable with their present configurations, a hurdle.

However, interoperability among future programs—and even between and among the pilot airports—is not actually a difficult issue if the pilots are viewed as testbeds for establishing the common, interoperable standard. Indeed, TSA, after testing the technology in the pilot programs, seems to have set a standard in Orlando that service providers will use for future RT programs.

TSA combined the use of iris images and fingerprint images, and in detail provided a technical spec for the operation of the program. Thus, to make the existing pilot programs interoperable with Orlando and future RT programs, the simplest way would be for pilot airports to require any RT service provider bidding to set up shop for a rolled-out private sector program to agree to reissue the existing members' cards for free in return for their having participated in the pilot. It is cheaper and easier than trying to create a software fix that will not be necessary in the future.

Put simply, interoperability is an obstacle easily overcome by taking the standards set by TSA in Orlando (or for that matter any modified standard that TSA sets once it sees how operations work in Orlando) and applying them to future RT programs.

Clearinghouse Structure

The second interoperability issue has to do with a clearinghouse that would combine the names of those enrolled in RT programs at various airports and by service providers. Someone enrolled in a program at O'Hare run by service provider A must be able to have his card recognized by a program at Tampa run by service provider B. Thus, a clearinghouse would be needed to collect the names of currently valid members and send them along with daily updates to all the kiosks run by all of the providers at all of the airports.

This represents a simple technology challenge, given that TSA has already set common membership criteria (it approves all members based on one standard), and apparently set the common technology standards for biometric capture and the smart card. The primary requirements of the clearinghouse would be meeting the strictest privacy and security requirements set by the service providers, having the trust and confidence of TSA, and the ability to do this without adding more than a few pennies of cost to the customer for this relatively simple task.

In short, with TSA having been active in the hard work of setting the technology and security standards, the path to interoperability is not nearly as difficult as it has been depicted.

AMERICAN SOCIETY OF TRAVEL AGENTS
Alexandria, Virginia, February 21, 2006

Hon. TED STEVENS,
Chairman,
Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Senator Stevens:

The American Society of Travel Agents (ASTA) applauds your efforts in holding the February 9, 2006 oversight hearing on commercial aviation security. ASTA wishes to go on record with respect to the Department of Homeland Security (DHS) Transportation Security Administration's (TSA) passenger screening programs Registered Traveler and Secure Flight. We ask that this letter become part of the official hearing record.

ASTA was established in 1931 and is today the leading professional travel trade organization in the world. Its current membership consists of approximately 5,800 travel agents across the Nation, with a total membership of 13,700 members in some 138 countries. ASTA's corporate purposes specifically include promoting and

representing the views and interests of travel agents to all levels of government and industry, promoting professional and ethical conduct in the travel agency industry worldwide, and promoting consumer protection for the traveling public.

Public confidence in our Nation's security is essential to the maintenance and growth of travel demand. Federal policies and practices can and do influence the demand for and the cost of delivering travel services. A careful balance between security and the flow of travelers requires passenger screening procedures to be free of unreasonable restrictions and obstacles that deter people from traveling. ASTA supports the permanent implementation of TSA's Registered Traveler program which will efficiently enhance the facilitation of the screening process for those frequent travelers who have voluntarily opted to qualify in advance.

In a related vein, the proposed regulations for Federal programs such as Secure Flight and the Centers for Disease Control and Prevention's Control of Communicable Diseases are major concerns for the travel agency industry. These programs are proposing the additional collection of passenger information and data by the private sector. The time has come for the U.S. Government to streamline and standardize passenger data collection across Federal agencies before any new regulations are adopted.

On behalf of the thousands of travelers that travel agents service throughout the year, we thank you again for your leadership role in reviewing the issues pertaining to passenger pre-screening in the post-September 11 world.

Sincerely,

KATHRYN W. SUDEIKIS, CTC,
President.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED STEVENS TO HON. EDMUND "KIP" HAWLEY

Question. Mr. Hawley, how much time and how much money have you spent on Secure Flight?

Answer. Exclusive of any spending for CAPPS II, some of which has also benefited Secure Flight, during the 18-months Secure Flight has been active, August 2004 through February 2006, the program has obligated $52.8 million in support of this effort. When spending on CAPPS II and projected obligations for Fiscal Year 2006, expected to total $42.2 million, are included, approximately $144 million has been obligated since November 2002.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED STEVENS TO CATHLEEN A. BERRICK

Question. Do you know the approximate number of man-hours and amount of funding that GAO has devoted to assessing the Secure Flight program?

Answer. Our review of the Secure Flight program, and of the Computer-Assisted Passenger Prescreening System II (CAPPS–II)—the predecessor to Secure Flight—have provided a detailed status of the programs' development and implementation to the Congress and have resulted in thirteen recommendations to the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) designed to help ensure the programs' successful implementation. In response to mandates contained in Fiscal Years 2004, 2005, and 2006 appropriations legislation,[1] and bi-partisan requests from eight Congressional committees, GAO has dedicated approximately 4.5 full time equivalent staff per year to review these programs since June 2003. During this time, we issued five reports, testified three times before several Congressional Committees, and provided numerous briefings to Congressional staff. Our work also contributed to several additional testimonies before Congressional Committees on TSA's overall efforts to strengthen the security of commercial aviation. TSA reported spending approximately $144 million on the development of Secure Flight.

As TSA proceeds towards implementation of Secure Flight, the FY 2006 appropriations legislation requires (1) DHS to certify that the program has addressed 10 areas related to the systems development and implementation and, (2) GAO to report to the Congress on DHS's certification of these issues no later than 90 days

[1] The Department of Homeland Security Appropriations Act, 2004, Pub. L. 108–90, § 519, 117 Stat. 1137, 1155–56 (2003); Department of Homeland Security Appropriations Act, 2005, Pub. L. No. 108–334, § 522, 118 Stat. 1298, 1319–20 (2004); and Department of Homeland Security Appropriations Act, 2006, Pub. L. 109–90, § 518, 119 Stat. 2064, 2085 (2005).

after DHS certification.[2] In accordance with this legislation, DHS can certify that Secure Flight has satisfied these 10 areas at any time either incrementally or in total, and does not have to wait for a GAO review to do so. Further, in an effort to be as constructive as possible, we have offered to provide to TSA the specific criteria we plan to use to review their certification of the 10 areas, and are exploring additional ways in which we can provide assistance to TSA as development progresses while maintaining our independence. We also appreciate the challenges TSA faces that are inherent in the development of a program such as Secure Flight, and will continue to work to minimize any impact our work may have on TSA as we conduct the remainder of our review.

[2] Section 518 of the FY 2006 Appropriations Act references the ten areas related to systems development and implementation listed in section 522 of the FY 2005 Appropriations Act.