IMPROVING PRE-SCREENING OF AVIATION PASSENGERS AGAINST TERRORIST AND OTHER WATCH LISTS

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JUNE 29, 2005

Serial No. 109–27

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

26–959 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

COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PETER T. KING, New York
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

DANIEL E. LUNGREN, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
CHRISTOPHER COX, California *(Ex Officio)*
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
PETER A. DEFAZIO, Oregon
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

IMPROVING PRE-SCREENING OF AVIATION PASSENGERS AGAINST TERRORIST AND OTHER WATCH LISTS

Wednesday, June 29, 2005

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY
Washington, DC.

The subcommittee met, pursuant to call, at 10:07 a.m., in Room 210, Cannon House Office Building, Hon. Dan Lungren [chairman of the subcommittee] presiding.

Present: Representatives Lungren, Cox, Linder, Pearce, Jindal, Thompson, Sanchez, Markey, Dicks, DeFazio, Lofgren, Jackson-Lee, and Pascrell.

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

The subcommittee is meeting today to assess the effectiveness of the systems and policies employed by the Transportation Security Administration for pre-screening air travelers.

I would like to welcome everybody to today's hearing. This morning, we will continue our oversight of the TSA by examining its aviation passenger pre-screening initiatives. By now, everyone should be acquainted with the current systems being used by the airlines to pre-screen passengers: The Computer–Assisted Passenger Pre-screening System, or CAPPS, and the no-fly list.

CAPPS is a rule-based system which flags air travelers for additional screening based on travel and ticket purchase habits. The specific elements of the program are classified, but many of the criteria are widely known and discussed.

Since the federal government mandated the use of CAPPS for airline passengers in 2001, we estimate that over 150 million passengers have been tagged by the system's overly broad system and unnecessarily subjected to the inconvenience and indignity of intrusive pat-downs and additional wandings.

We have all personally learned of many instances where TSA has aggressively searched grandmothers, disabled veterans, small children, and others who appear to pose minimal risk to the homeland security of this country as a result of CAPPS.

The watch lists, which are the focus of today's hearing, also have their own problems. By some estimates, 2 out of every 100 flyers have been misidentified as persons on these lists. If true, that is

a lot when we are dealing with 1.8 million passengers every day. The system of watch lists currently in use does not have an adequate redress process for those who have been misidentified time and time again. None of the watch lists used by TSA utilizes the complete set of databases available within the federal government.

To some of us, the current regime seems to make little sense. It appears to hassle travelers, waste resources and has no measurable benefit to aviation security, at least not a benefit that TSA has demonstrated to us yet. TSA has been working for some time to replace CAPPS and improve watch list matching with some progress, but TSA's latest effort to secure flights seems to be running into difficulties that will delay its implementation.

This is not good because the longer we delay, the longer we have the current system, which is certainly not as good for our security, our privacy or our pocketbooks.

I am also concerned that TSA has no plans to make CAPPS more effective and less of an imposition on the traveling public even after a Secure Flight is in place, when it is in place.

TSA must continue its development of an effective targeted passenger pre-screening system to improve its aviation security operations and reduce costs. It must also integrate all pre-screening initiatives to minimize redundancy and enhance efficiency. Congress must do the oversight along the way as well. We must make sure we are not standing in the way of getting this new system in place as quickly as possible.

Today, we will hear from two distinguished panels of witnesses to gain the insight of passengers, airlines, other stakeholders and the Department itself about the problems with the current system of passenger pre-screening and how we can improve it.

Mr. I thank all of our witnesses for appearing before us today, and I recognize the ranking member of the full committee, Mr. Thompson, from Mississippi, for any statement he wishes to make.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I look forward to the testimony of the witnesses today on this very important subject.

Millions of Americans flying this summer continue to be screened under CAPPS I, the behavior-based terrorist screening system run by the airlines that is designed to root out terrorists before they board commercial aircraft. The airlines will likewise continue to use TSA's no-fly and selectee list as an additional tool to keep passengers safe.

But change is supposedly coming to improve and perhaps replace these systems. TSA has set a deadline to begin a test run of the new Secure Flight Program this August. Secure Flight will check all passengers against TSA's consolidated watch list, a watch list that fuses together numerous federal terrorist watch lists.

The TSC watch list is supposed to represent the most up-to-date listing of known and suspected terrorists, but a recent report by the Department of Justice's IG's Office raises significant concerns as to how accurate and complete the TSC's watch list actually is. If the TSC's list cannot be trusted, then Secure Flight may not work either.

Another concern in recent weeks has been a possible violation of the Privacy Act by TSA. In September, TSA said that it would, on

a very limited basis, test the use of commercial data against a secure flight record system. TSA also indicated that it would not store the commercially available data that it would use for testing. Several weeks ago, we learned that neither of these representations were true.

Finally, we recently learned that even if the Secure Flight issues are addressed, TSA may require the airlines to continue running CAPPS I Program, a burden the airlines I believe should not have.

I hope that Mr. Oberman will address these issues. Furthermore, I hope that he can discuss whether money is going in Secure Flight and what we have gotten in past funds spent. For example, $71.5 million was paid to a contractor for the pay of CAPPS II Program, and another $8.2 million was paid for its work on Secure Flight before it stopped working on the program. If the Department had only listened to Congress and built privacy into CAPPS II, it probably could have saved a lot of this money.

In short, I am very concerned, Mr. Chairman, that Secure Flight may be off track. According to the GAO, Secure Flight was supposed to have a final concept of operation and definition of requirements, including whether it was going to use commercial data, by March and April, respectively. The date by which Secure Flight was supposed to be fully operational on two carriers has already slipped by 4 months. We need serious answers where this program is going. If we do not get answers, Secure Flight may suffer the same fate similar to CAPPS II. It may never leave the gate.

Mr. Chairman, I yield back.

Mr. LUNGREN. I thank the gentleman.

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

PREPARED OPENING STATEMENT OF THE HONORABLE CHRISTOPHER COX, A REPRESENTATIVE IN CONGRESS, FROM THE STATE OF CALIFORNIA, AND CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

Thank you, Mr. Chairman.

Screening passenger manifests for potential terrorists is one of the most important and potentially most effective aspects of our aviation security system—because instead of focusing on knifes, nail clippers, and other countless potential weapons, or children and grandmothers, we are focusing on the more finite universe of known and suspected terrorists. The problem is not with the concept—but with its execution to date, which is carried out not by TSA, but by the airlines under difficult circumstances.

According to TSA, roughly two percent of all travelers have names that are on or closely resemble names on the Terrorist Screening Center watchlists. In other words, more than 13 million passengers annually—or some 36,000 per day—are misidentified by the current system, and are inconvenienced by costly and time-consuming extra security procedures or completely prevented from flying. That does not even count the millions more who are flagged for secondary screening not because of their name, but because they purchased a ticket in a manner that TSA has determined raises a suspicion of terrorism—the system known as CAPPS.

The poor souls who wish to have their good names cleared from the watchlists have to navigate mountains of TSA red tape and bureaucracy to get on a "cleared" list that may or may not prevent them from being flagged as terrorists by the airlines on future flights—depending on the particular airline's particular procedures. One of our witnesses, former Congressman and Presidential candidate John Anderson understands this problem all too well—since he is one of those unlucky passengers whose name matches or closely resembles a name on the terrorist watchlist. With a name like that, I assume there are thousands of other John Anderson's facing this problem on a daily basis.

While these facts alone should be enough to question the efficacy of the current system, further examination shows that the airlines are not provided the most com-

prehensive terrorist watchlist due to security concerns. They also do not receive certain related information on these suspected terrorists that could help reduce misidentifications and more promptly resolve close matches.

As a result, we have a system that flags millions of innocent people for extra screening or security procedures without cause, and we may actually be missing some people with terrorist affiliations.

Over the past year, TSA has been attempting to address these inadequacies through the development of the Secure Flight program, as mandated by Congress in an overwhelmingly bipartisan fashion last year. Under this system, TSA will assume from the airlines the responsibility for managing the terrorist watchlist matching function.

From what we can tell, TSA is mostly on the right track. Secure Flight will rely on expanded passenger name records, improved name-matching software, and the TSC's full database of known or suspected terrorists. It will also have improved passenger redress capabilities, making this function more expedited and more uniform. These steps should significantly minimize the ambiguities that have resulted in the thousands of daily false positives, while also improving our ability to find real terrorists.

While there remain a host of important issues involving Secure Flight to be worked out, Congress must be mindful not to let the perfect be the enemy of the good—or the enemy of the worse. The current system is a terrible waste of resources, is an unjustified imposition upon passengers' privacy rights and freedoms, and is of questionable security benefit. Secure Flight must be implemented as quickly as possible, with appropriate safeguards, so we can move beyond what is in place today.

I would like to thank the witnesses for appearing today and for providing their insight on this important issue.

Mr. LUNGREN. We are pleased to have two expert panels of witnesses here today to give testimony on this important topic. Let me please remind the witnesses that your entire written testimony will appear in the record, and we ask you to limit your oral testimony to the 5-minute period allotted.

The Chair now with pleasure recognizes the Honorable John Anderson, the distinguished former member of the House of Representatives, candidate for the presidency in 1980, may I just say that during my first tour of duty here in Congress, he was one of the first members of the leadership that I met. It seems like it was just yesterday, although it was 1979.

Congressman Anderson, it is our pleasure to have you speak now.

STATEMENT OF THE HONORABLE JOHN ANDERSON, A FORMER REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. ANDERSON. Thank you very much. And I also appreciated very much the statement read just a moment ago by the chairman of the full committee with respect to the importance of the hearing that you are holding this morning.

I am here to present some anecdotal evidence of a personal experience that is relevant I think to the scope of your inquiry.

Earlier this year, I made two trips abroad on the 23rd of March without any trouble. I boarded a flight in Fort Lauderdale, Florida and flew to Amsterdam on a personal family visit with a daughter who resides there and then returned after 10 days to begin preparations for a trip that was organized by former Members of Congress and coordinated by the Council on Excellence in Government, designed to bring former members like myself to universities in other countries, in this case Germany. And they had scheduled a flight from Washington to JFK and from JFK to Frankurt Am

Rhein and then a schedule that would bring us to about five different German cities to converse with members of the faculty and the student body of those institutions.

Shortly before the second flight was about ready to go, I was told, "You will have to go to the airport personally some days in advance because you are on the watch list. You are one of those suspected of possible terrorist activity and of interest to the government, a person of interest." Well, flattering as it is to be a person of interest, I was a little bit shocked to find myself included in that group.

So my first thought was for the first time in 25 years, I will seek the aid of my congressman who now happens to be Clay Shaw. I am a legal resident, registered independent voter in the State of Florida. I went to Clay's office and he promptly undertook an investigation and very shortly produced a satisfactory result.

But I was encouraged to appear this morning to—well, I should tell you what I had to do. It was not quite just as simple as talking to Clay Shaw and his staff, although they were most helpful.

I supplied, with the assistance of the staff, four items of identification, including my registered voter's card from the State of Florida, my driver's license, issued by that state, my U.S. passport, which was in good order, and then hopefully also my former Member of Congress card would throw some weight into the balance, and some days later received a communication from the Office of the Ombudsman saying that following the receipt of my passenger identity verification form, PIV, and their subsequent investigation, the TSA has verified your identity, and, accordingly, we have provided sufficient personal information to the airlines to distinguish you from other individuals in the system in issuing your boarding pass more efficiently.

Then there was a paragraph that followed that said, "Notwithstanding, you should have certain documents, one or more, to help expedite receipt of a boarding pass," and that the airline "might require a brief period of time to verify your information. The process should not result in extensive delay."

On the day the flight was scheduled to leave, I very pessimistically arrived 3 hours ahead of time at Delta Airlines. Fortunately, since I was a business class traveler, I could luxuriate in the surroundings of a nice lounge but finally boarded.

My concern today is for less fortunate travelers without a congressman and his staff to get through quickly to the right person in TSA. Suppose it was someone who was booking a last-minute flight in response to a family emergency. You wanted to be at the bedside of a dying mother or other family member. How well could that hypothetical traveler cope with the kind of requirements that apparently now are sufficient to put you on this list?

I raise these questions, and this is not in high judgment and high designation. I appreciate what the chairman said, it is important to identify terrorists before they board an aircraft, and there have to be some procedures in place, but should not the TSA have procedures in place that anticipate the difficulty that I have only cursorily outlined, and have they kept this committee and others who have a valid interest properly informed as to what criteria they employ to put a person's name on a list of a possible suspect of terrorist activity?

All kinds of lists in this country, best dressed people, most highly compensated chief executives, but when the government starts preparing lists, they ought to be very careful, it seems to me, any government agency, who it is they include.

And, believe me, this is the first time I have ever done this. Last night, I just had the idle thought cross my mind, I wonder, oh, what Google would say about me. So I said to my wife sitting there at the home desktop computer, "Google in John B. Anderson and see what comes up." Well, I have sheet of papers here, I think there are 16 pages in all, about John B. Anderson, me—the books that I have written, the articles that I have written, the places I have visited, et cetera, et cetera, more than you would ever want to know.

So if I could find that out that quickly, why should not some simple Googling of it—and I appreciate the fact that I have a common surname. This has bothered my son who has had to suffer some of the indignity because he is John B. Anderson, Jr. But if we can that easily acquire a load of information about who we are and distinguish us from other John Andersons and when I have closed a real estate deal in Washington from time to time, I have had to endure the fact that there are few John Andersons with judgments against them that I had to explain.

So I can see that there is a problem with people with a fairly common surname, but I think the ease with which I was able to produce the kind of information that ought to help the Agency decide whether or not to include that name along with a lot of other people on the no-fly list probably needs some reexamination.

Thank you, Mr. Chairman.

[The statement of Mr. Anderson follows:]

PREPARED STATEMENT OF HON. JOHN B. ANDERSON

Mr. Chairman, Ranking Member Thompson and members of the Subcommittee, I am pleased the Committee has undertaken this review of the Transportation Security Agency's establishment of a no-fly list in its regulation of air transportation.

Earlier this year, I accepted the invitation of the Former Members of Congress Association, a group of which I am a member, to travel to the Federal Republic of Germany under a program which they were conducting with the aid of the German American Marshall Fun and coordinated with the assistance also of the Council on Excellence in Government.

Our itinerary embraced cities like Frankfurt Am Rhein, Cologne, Bonn, Frankfurt Am Oder and Berlin. It involved visits to German Universities and contacts with both their students and faculty.

Some days before our departure on April 23, 2005, the group arranging my ticketing notified me and travel arrangements that I was on a no-fly list and Delta Airlines would not issue the ticket prior to the departure date until my status was clarified.

As a registered voter for some years now in Florida, I contacted Congressman Clay Shaw's office, went to his office on Capitol Hill and with the help of his staff,submitted four items of identification including, voters card, drivers license, passport, former Members of Congress identification card and some days later received a communication from the Office of the Ombudsman saying that following the receipt of my Passenger Identity Verification (PIV) Form and their subsequent investigation "the TSA has verified your identity.

Accordingly, we have provided sufficient personal information to the airlines to distinguish you from other individuals and assist them in issuing your boarding pass more efficiently."

The following paragraph said that not withstanding this you should have certain documents, one or more, to "help expedite receipt of a boarding pass" and that the airline "might require a brief period of time to verify your information but the process should not result in extensive delay."

My concern today is for less fortunate travelers without a Congressman and his staff to get through quickly to the right person at TSA. If the flight booking was in response to a family emergency or for some other reason where delay would be serious, how well can that hypothetical traveler cope? If the person with a common surname arrives at the airport ticket counter without the availability of the expeditious advance work of someone like my friend Congressman Shaw, how well would they fare? Should TSA have procedures in place that anticipate the difficulty I have only cursorily outlined. Why should not persons identified by TSA as being ?of interest, and possible connections with terrorist activities be forewarned? Has TSA kept this committee and others who have a valid interest properly informed as to the standards they employ in describing someone as a person of interest to law enforcement authorities, and therefore a candidate for the "no-fly list"?

Mr. Chairman, I again appreciate this opportunity to provide written testimony.

Mr. LUNGREN. I thank the gentleman for his testimony.

I might just mention to the gentleman for the record that we were contacted by the congressional office in your particular case, and the lady sitting directly behind me, Ms. Winsome Packer, handled that, but I might say she worked on it for about a week with TSA to go through all the steps. And as you suggest, I doubt most Americans would have that ability or time to do that sort of thing, particularly under the circumstances you mentioned.

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

Mr. LUNGREN. Yes, I will.

Mr. DICKS. As I understand it, even after you do all that—I have had three of four constituents of mine with very similar names, Thompson, for example, and even once you have gone through all it, which you have done, you still have to go in early and report to the desk because they have got to go through this and check you out again the next time you fly.

Mr. ANDERSON. I think that is true. The letter from TSA suggests as much, that you should be prepared with one or more forms of identification, which to me indicates that I probably would still have some delay, but hopefully they say it is not going to be extraordinary.

Mr. LUNGREN. Well, the good news, John, is you are not forgotten.

[Laughter.]

Mr. ANDERSON. That I appreciate.

Mr. LUNGREN. I thank you for your testimony.

The Chair now recognizes Mr. James May, president and chief executive officer of the Air Transport Association, to testify in his statement for 5 minutes.

STATEMENT OF JAMES MAY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, AIR TRANSPORT ASSOCIATION

Mr. MAY. Thank you, Mr. Chairman.

In 2001, the Air Transport Association pledged its support of appropriate government efforts to utilize available information to improve the effectiveness and the efficiency of passenger pre-screening. As we said then, we believe that a security system premised on looking at people, not at things, is most likely to produce the results that we all need.

Four years later, things have not progressed as far as any of us would have hoped. The list of programs that never quite came to fruition goes on as we keep circling the same issues: CAPPS I, CAPPS II, Registered Traveler, Secure Flight. We could go on with

a long list of those programs that have not yet quite come to fruition.

And so I think it is time for this committee to push TSA to either fish or cut bait and make the changes that are necessary to these programs.

We are cautiously optimistic that TSA reports of progress in the development of Secure Flight, however. We see Secure Fight as improving both the quality of security and the passenger experience, and I think it has the potential, at least, to reduce the number of times that Mr. Anderson would have to go through an unfortunate experience, as he did.

There remain some very challenging implementation issues ahead, but I think the picture does hold promise. This can only be made to work, however, if there is real leadership from this committee, the Congress and the administration as to what it will take. Let me give you a couple of thoughts on the challenges.

First, I think we need agreement on data collection, not just for Secure Flight, but across the entire spectrum of Department of Homeland Security agencies. We need consistent, not duplicative or competing requirements. If CBP, the Customs and Border Patrol people, are going to collect information for one program, then TSA ought to have a very consistent collection format for their programs.

Secondly, I think it needs to be understood that this is a massive undertaking and that sufficient time and resources need to be made available to resolve any of an array of technology, operational, economic and policy questions which are presented, not the least of which is privacy.

And third, action has to be taken by government to eliminate the unnecessary selection of passengers due to poorly maintained and poorly vetted lists. That is exactly what Mr. Anderson talked about.

Finally, in order for Secure Flight to succeed, TSA must negotiate some extremely challenging privacy issues, as it looks to developing information management as a tool against the threat of aviation terrorism. To assist the process, Congress should be clear as to precisely what privacy issues need to be addressed, and there must be a clear and effective resolution of international privacy concerns.

As I said, we are optimistic about the potential for Secure Flight. We think it warrants real support, but there are many challenges ahead.

Having said that, while we believe there could also be merit in a voluntary traveler identification program, we are not persuaded of the merits of what has become the Registered Traveler, or RT Program. And I think the problem is that TSA has never been able to provide a definition of program participation benefits. They remain ambivalent as to whether or not this should be a true security program or some type or passenger perk program. In our judgment, to be successful, we need to know what exactly the program will provide participants, and it must be a true security program as well. Without that information, I think RT is going to be a nonstarter.

And, finally, I would like to address the issues presented by the concept that has come to be known as APIS–60. Under this pro-

gram, passenger passport data is batched and transmitted to the government within 15 minutes of departure of U.S.-bound international flights. Now, that information is used to vet passengers prior to arrival.

In the post–9/11 world, DHS and others have expressed a strong interest in receiving APIS data 60 minutes prior to the flight's departure. We have been engaged with CBP and others to improve that process.

I will not go into the complexities, but the bottom line is that if we are required to present information 60 minutes in advance of departure when we frequently only get it a half hour in advance of departure for many connecting passengers, it is a program that is doomed to fail.

We have looked for alternatives that will address both security and operational concerns, the most desirable approach in our view would be to develop a real-time interactive "go/no-go process." There is a program that the Australians and the New Zealanders have had in effect, the Canadians are about to adopt it, that we think provides the model.

In conclusion, Mr. Chairman, I would like to emphasize three critical points. First, the airlines industry commitment to security is absolute. Second, we applaud and endorse Congress' recognition that aviation security is national security and ought to be funded accordingly.

Third, and finally, we urge this committee to push aggressively to streamline, simplify and consolidate the multiple, diverse but heretofore uncoordinated programs requiring collection of passenger information. These programs must be harmonized in order to best leverage the available information and investment. We would also encourage a review of the Privacy Act restrictions to be certain they provide an appropriate framework for dealing with post–9/11 and security concerns.

Thank you.

[The statement of Mr. May follows:]

PREPARED STATEMENT OF JAMES C. MAY

In November of 2001, the Air Transport Association pledged its support of appropriate government efforts to utilize passenger information and available government and public data to improve both the effectiveness and the efficiency of passenger pre-screening. As we said then, and have heard echoed repeatedly since, we believe that a security system premised on "looking at people and not things" is most likely to produce the results we all need. At that same time, we called for the establishment of voluntary traveler-identification program to further expedite security processing for those opting to participate. We remain convinced that both programs have significant potential in terms of further improving the level of security, maximizing the utility of Transportation Security Administration (TSA) resources and enhancing passenger convenience.

Now, however, almost four years later, while we remain committed to these goals, it is no secret that things have not progressed as far as any of us would have hoped. CAPPS II, Secure Flight, Known Traveler, Registered Traveler—the list of programs that never quite come to fruition goes on, as we keep circling the same issues. In our view, it is time as they say ?to fish or cut bait.?

We are cautiously optimistic at TSA reports of real progress in the development of Secure Flight. We see Secure Flight as a very valuable addition—improving both the quality of security and the passenger experience. There remain, by universal acknowledgement, some very challenging implementation issues ahead but the picture right now holds promise. This can only be made to work, however—to come to a different end than its multiple predecessors—if there is real leadership from this committee, the Congress and the administration. We are committed to a successful

Secure Flight program—but we must have the leadership commitment to getthis done.

As to what it will take to make this work, let me provide you with a few thoughts on the challenges:

First, we need agreement on data collection—not just for Secure Flight, but across the spectrum of Department of Homeland Security (DHS) agencies. We need consistent, not duplicative or competing, requirements and it must be clear that **all** participants in the reservation process share data-collection obligations, including travel agents and Global Distribution Systems;

Second, it must be clearly understood that this is a massive, very challenging undertaking and that sufficient time and resources must be available to bring a successful outcome; this includes a complete and cooperative analysis and implementation agreement treating an array of technological, operational, economic and policy questions that must be resolved by both government and industry before *any* final decisions are made. This cannot work with unreasonable timelines or mandates;

Third, whether we are dealing with names of interest under an eventual Secure Flight program, or the current Watch List system, action must be taken by the government to eliminate the unnecessary selection of passengers due to poorly maintained and poorly vetted lists. Names on any list should only be there with good and sufficient reason. Steps in this direction are currently underway, however, this process must be completed and institutionalized going forward; and finally, in order for Secure Flight to succeed, TSA must negotiate some extremely challenging privacy issues as it looks to developing information management as a tool against the threat of aviation terrorism: To assist the process, Congress should be clear as to precisely what privacy issues need to be addressed to fully protect legitimate passenger interests and yet still permit appropriate uses of data. On a related front, there must be a clear and effective resolution of international privacy concerns before implementation.

As I said, we are cautiously optimistic about the potential for Secure Flight and see it as a vast improvement over the current Watch List protocols—from a security perspective, from a service perspective and from a privacy perspective. In our judgment, it warrants real support.

Having said that, while we believe there *could* also be merit in a voluntary traveler identification program, we are not persuaded at this point of the merits of what has come to be called "Registered Traveler (RT)." The problem is fundamental—the TSA has never been able to provide a definition of program participation benefits. TSA remains ambivalent as to whether this should be a true security program or some type of passenger "perk." In our judgment, to be successful, we need to know exactly what the program will provide participants. Those benefits must be interoperably available at all airports and it must be a true security program. Until it is known exactly what is intended, with specificity, it is not possible to quantify the value of an RT program—or, as a result, get any real understanding of the appropriate size of *any* investment in its development. Without this information, RT is a non-starter and warrants no further attention until these fundamental questions are answered.

Finally, I would like to address the issues presented by the concept that has come to be known as APIS–60. For those not acquainted with this issue, it arises from a long-established legacy Customs and Immigration Advanced Passenger Information System program. Under that program, passenger passport data is batched and transmitted to the government within fifteen minutes of departure of U.S.—bound international flights, for vetting prior to arrival.

In the post-9/11 world, DHS and others have expressed strong interest in receiving this data—which would be cross-checked with various watch lists—sixty minutes *prior* to a flight's departure. Since we first learned of the government's interest in such a program in March of 2004, we have been engaged in extended discussions, testing and exploration of the issue with DHS and its Customs and Border Protection experts.

While in the interest of time, I will not detail the complexities of this issue, at an elementary level the problem is that the airlines typically do not have reliable passenger passport data until the passenger presents his or her documents at check-in. Uninformed or unrealistic demands for this information prior to departure could be exceptionally destructive.

While many international travelers do arrive two hours or more in advance of a flight, late-arriving passengers, particularly connecting passengers, may not present themselves until minutes before departure. As a result an APIS–60 requirement would significantly impact industry operations and economics on a global scale, either through massive schedule inefficiencies or, more likely, by "disconnecting" passengers on a wholesale basis.

Because of these functional realities we have looked for alternatives that will address both security and operational concerns. The most desirable approach, in our view, would be to develop a real-time, interactive, "go/no-go" process that would permit passport data to be swiped and transmitted, and an answer provided on the spot—not unlike approval of a credit-card transaction. The Australian government utilizes a process along these lines for pre-approving passengers traveling to Australia from anywhere in the world. While, without question, the scale of travel to and from the United States is orders of magnitude larger, and a U.S. system would be significantly more complex, we believe this real-time approach would be infinitely more practical than any alternative. Should that prove unworkable, however, we believe that other alternatives should be explored including "rolling" transmissions of APIS data as a flight builds to departure—leaving only a modest percentage of passengers for last-minute clearance or, conceivably, an earlier collection of APIS data. We recently advised Secretary Chertoff of our commitment to working with the department to develop a practicable solution and, we remain committed to this goal.

In conclusion, I would like to emphasize three critical points:

First, the airline industry's commitment to security is absolute—we fully recognize that the security and safety of our operations must be unquestionable; at the same time, we are committed to the protection of our customers' legitimate privacy interests.

Second, we recognize that, particularly with regard to security, Congress's recognition that aviation security *is* national security necessitates the government's integral involvement in our business. This in turn, necessitates our common reliance on strong professional leadership that understands the imperative for fully integrating security into the complex, but essential, provision of air transportation. Fortunately, with the leadership team in place at the Department of Homeland Security and the anticipated return of Mr. Hawley to direct TSA, we have the administration?s leadership team uniquely well-positioned and;

Third and finally, we urge this committee, working with the full Congress and the administration, to push aggressively to streamline, simplify and consolidate the multiple, diverse—but heretofore uncoordinated—programs requiring collection of passenger information to facilitate one or another security goal. These programs must be harmonized in order to best leverage the available information and investment, and they may also warrant consideration of a review of Privacy Act restrictions to be certain they provide an appropriate framework for dealing with post-9/11 privacy and security issues.

Thank you for the opportunity to appear before you today. I will be happy to respond to questions.

Mr. LUNGREN. Thank you, Mr. May.

The Chair would now recognize Mr. Paul Rosenzweig, the senior legal research fellow at the Heritage Foundation, for his testimony.

STATEMENT OF PAUL ROSENZWEIG, SENIOR LEGAL RESEARCH FELLOW, CENTER FOR LEGAL AND JUDICIAL STUDIES

Mr. ROSENZWEIG. Thank you very much, Mr. Chairman, and thank you for the invitation to appear.

As a lookout, I should note at the beginning that I also serve on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, but nothing I say here is that Committee's view. I speak for myself only.

I would like to step back a minute and reflect where we were 20 years ago. Twenty years ago, you could get on a shuttle flight to New York from Washington and fly without showing any identification and pay cash. You could fly anonymously, essentially. I think it is impossible to imagine returning to that system for obvious national security reasons, and aviation is, as Mr. May said, part of national security.

So the bottom line is we need to identify people who fly, and we do that today. The question is whether or not we are doing it the right way and whether or not we can do it better. Today, I would

submit we are doing it in a way that is no longer terribly effective. We have a CAPPS I system that uses behavioral rules that, as the chairman said in his opening, are fairly well known outside of TSA and thus fairly ineffective and fairly easy to avoid. And we have a no-fly list watch matching system that, as Mr. Anderson's experience shows, is ineffective and catches the wrong people.

Why does the current system not work? Well, first, because of national security concerns, we cannot share the full TSC watch list with the airlines who are currently responsible for doing the matching. Second, each airline administers the watch list differently, and so there is no single common standard for defining what is in fact a watch list match.

Third, each airline uses different automated matching programs, they use different computer programs and different systems. So there is actually a high variability in who gets matched. Who gets matched at Delta may indeed be different than who gets matched at American, and certainly amongst the smaller airlines.

And, finally, because the lists are administered in the end by the airlines, there is no single system or standard list of cleared passengers so that they cannot propagate the list of clearances—like the clearance for Mr. Anderson—cannot propagate out to the airlines effectively.

The current system that we have in place of the no-fly list is inefficient, both because it inconveniences innocent travelers like Mr. Anderson but also because it is a waste of resources. Every time we spend time clearing Mr. Anderson again or subjecting someone in his situation to additional secondary screening, we are wasting time and money of TSA screeners that ought to be directed at those who are truly ambiguous on potential threats.

Thus, I think that the testing program that we are undertaking now to see whether or not a more refined watch list can be used is the right way to go. Preliminary results are at least suggestive of success. With the addition of a simple date of birth field, it is estimated that we can reduce the number of matches on the watch list by roughly 60 percent. If that is true, if that actually proves to the be the case, that would be a huge success. It would reduce from roughly 35,000 to 14,000 a day the number of people who are in this close match list, not secondary screenings but for people who are really people of interest. And if we can do that, that would be a great thing.

Now, the system is obviously undergoing testing. We have not determined yet whether or not this proof of concept can be implemented in a broader range, addressing 1.8 million passengers per day, and we also need to get right issues like Privacy Act notice disclosures, like Mr. Thompson mentioned, and a fully integrated redress procedure so that when Mr. Anderson goes through the process once and gets cleared, that should be the end of it.

We need to develop the technological system of tethering information back to its original source so that when the correction is entered, Mr. Anderson, with the addition of his date of birth or some other uniquely identifying number, becomes a cleared person who can sail through without any additional clearing.

That is technologically possible, I believe, and it is ahead of us. Are we there yet? I do not think so. But is the Secure Flight Pro-

gram a promising alternative to our current system, which I think everyone agrees is only somewhat functional? Absolutely.

So I commend the committee for its attention to the program, and I commend it for staying on top of TSA in monitoring its implementation of the program as we go through testing.

Thank you very much, Mr. Chairman.

[The statement of Mr. Rosenzweig follows:]

PREPARED STATEMENT OF PAUL ROSENWEIG

THE HERITAGE FOUNDATION

Good morning Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to testify before you today on the challenge of maintaining the balance between security and constitutionally protected freedoms inherent in responding to the threat of terror, in the particular context of the Transportation Security Administration's (TSA's) proposed Secure Flight system.

For the record, I am a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation, a nonpartisan research and educational organization. I am also an Adjunct Professor of Law at George Mason University where I teach Criminal Procedure and an advanced seminar on White Collar and Corporate Crime and I serve on the Editorial Board of the Journal of National Security Law and Policy.

I am a graduate of the University of Chicago Law School and a former law clerk to Judge R. Lanier Anderson of the U.S. Court of Appeals for the Eleventh Circuit. For much of the first 13 years of my career I served as a prosecutor in the Department of Justice and elsewhere, prosecuting white-collar offenses. During the two years immediately prior to joining The Heritage Foundation, I was in private practice representing principally white-collar criminal defendants. I have been a Senior Fellow at The Heritage Foundation since April 2002.

I should also note that I serve as Chairman of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. This group is constituted to advise the Secretary and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that affect individual privacy, as well as data integrity, data interoperabilty and other privacy-related issues.

Nothing in my testimony, oral or written, reflects the views of the Privacy Advisory Committee or any other member of the Committee. My own views, however, are certainly informed by my service on that Committee and the information I learn there. We heard testimony earlier this month, for example, at a hearing in Boston, about many of the Department's screening programs, including Secure Flight.

More broadly, my perspective on the question before you is that of a lawyer and a prosecutor with a law enforcement background, not that of technologist or an intelligence officer/ analyst. I should hasten to add that much of my testimony today is based upon a series of papers I have written (or co-authored) on various aspects of this topic and testimony I have given before other bodies in Congress, all of which are available at The Heritage Foundation website (*www.heritage.org*). For any who might have read portions of my earlier work, I apologize for the familiarity that with attend this testimony. Repeating myself does have the virtue of maintaining consistency—I can only hope that any familiarity with my earlier work on the subject does not breed contempt.

In this testimony, I want to do four things: summarize the history of the Secure Flight program; discuss the anticipated utility of Secure Flight and the most controversial aspect of its architecture, the possible use of commercial data to verify identity; discuss privacy impact compliance as a necessary condition for implementation; and finally, discuss the question of redress.

I. A Bit of History

One common critique offered by skeptics of new initiatives to combat terrorism is the concern that advances in information technology will unreasonably erode the privacy and anonymity to which American citizens are entitled. They fear, in effect, the creation of an "electronic dossier" on every American. Attention to this issue has particularly focused on TSA's proposal to use an enhanced information technology program to screen airplane passengers. That program, known as Secure Flight, is intended to identify every passenger to determine his or her presence on a watch list for screening or to be denied access to the plane.

Since September 11th the aviation industry has undergone many changes to strengthen airport security. The TSA was created and placed in charge of passenger and baggage screeners (who are now federal employees). It has been using explosives detection systems on 90 percent of checked baggage and substantially expanded the Federal Air Marshal Service. However, little has been done to determine whether a person seeking to board an aircraft belongs to a terrorist organization or otherwise poses a threat. In order to meet this objective, the Transportation Security Administration is developing the Secure Flight.

Most of the changes made in airport security have focused on looking for potential weapons (better examination of luggage, more alert screeners) and creating obstacles to the use of a weapon on an aircraft (reinforced cockpit doors, armed pilots, etc). A computer-aided system would improve the TSA's ability to assess the risk a passenger may pose to air safety.

CAPPS I: The original, limited CAPPS I system was first deployed in 1996 by Northwest Airlines. Other airlines began to use CAPPS I in 1998, as recommended by the White House Commission on Aviation Safety and Security (also known as the Gore Commission).[1] In 1999, responding to public criticism, the FAA limited the use of CAPPS I—using it only to determine risk assessments for checked luggage screening. In other words, between 1999 and September 2001 CAPPS I information was not used as a basis for subjecting passengers to personal searches and questioning—only for screening checked bags. As a consequence even if CAPPS I flagged a high-risk passenger he could not be singled out for more intensive searches.

After September 11 CAPPS I returned to its original conception and is now again used to screen all passengers along with their carry-on and checked luggage. However, the criteria used to select passengers, such as last-minute reservations, cash payment, and short trips are over inclusive. This is a very crude form of pattern-recognition analysis. So crude that it can flag up to 50% of passengers in some instances, mainly in short haul markets.[2] These criteria are also widely known and thus readily avoided by any concerted terrorist, effort. Nor does CAPPS I attempt to determine whether or not the federal government has information that may connect a specific perspective passenger with terrorism or criminal activity that may indicate they are a threat to the flight. And it is costly—I've heard informal estimates as high as $150 million per year for domestic airlines to operate the system. As a result, we are wasting resources: it's likely that if Osama bin Laden tried to board a plane today CAPPS I would not identify him for arrest or further inspection.[3]

The Current System: In the immediate aftermath of September 11 it quickly became obvious that the failure to make any matching effort was problematic. The existing watch lists were disjointed and inconsistent and could not be effectively shared with airlines (for fear of disclosing sensitive or confidential national security information). But some watch list matching was, rightly, deemed necessary.

To meet that perceived need the Administration took two steps. First, it created the Terrorist Screening Center in an effort to consolidate and coordinate the multiple government-wide watch lists. Second, the Administration created a system whereby watch list names were shared with individual airlines for them to match against their own customer lists.

This current system is problematic for several reasons:

- Most saliently, because of the national security sensitivity of the watch lists only a portion of the lists can be shared;
- Because each airline administers the watch list matching differently, there is no single common standard for defining a watch list "match";
- Because each airline uses different automated matching programs, there is a high variability in the matching operational methodology; and

---

[1] *See* White House Commission on Aviation Safety and Security (Feb. 12, 1997) (avaiable at *http/ /www.airportnet.org/depts/reguatory/gorefinaL.htm*).

[2] *See* Robert W. Poole, Jr. & George Passatino, "A Risk-Based Aiort Security Policy" Reason Public Policy Institute at 11 (May 2003).

[3] It has been reported that the CAPPS I system was partially effective, flagging nine of the 19 September 11 terrorists for additional screening. *See* National Commission on Terrorist Attacks Upon the United States, "The Aviation Security System and the 9/11 Attacks: Staff Statement No.3" (Jan. 27, 2004) (available at *http://www.9–11commssion.gov/hearings/hearig7 /staff statement 3.pdf*]); *see also* Sara Goo and Dan Eggen, "9/11 Hijackers Used Mace and Knives,Panel Reports," Wa. Post at A1 (Jan. 28,2004) (summarizing report). To the extent that is true it emphasizes both that some form of screening can be effective, that the limitation to bag-only screening was unwise, and that however effective electronic screening might be, the human element will always be a factor in insuring the success of any system.

• Because of differing programs and standards a list of "cleared" passengers who are on the watch list cannot be readily propagated throughout the system (no doubt the cause, for example, of Senator Kennedy's persistent screening).

Recognizing the inadequacy of the system and the waste of resources that attends the disutility of screening those who do not need to be screened, TSA began developing potential replacement systems. In the post-9/11 world the question is not really whether we will watch list match, but how best to do it.

CAPPS II Proposed: The TSA reasonably believes that screening what a passenger is carrying is only part of the equation and began developing CAPPS II as a successor to CAPPS I in order to determine whether the individual poses a threat to aviation security. CAPPS II was intended to use government intelligence and law enforcement information in order to assign risk levels to passengers based on real information not arbitrary models. The TSA would then be able to devote more of its resources to those with a higher score (indicating they pose a greater risk), than those deemed to be a lesser concern (although some degree of randomness will need to be retained).

In January 2003, TSA released a Privacy Act notice for CAPPS II, the successor to CAPPS I.[4] Many critics raised substantial concerns. Some thought that CAPPS II, as originally proposed, was too broad in scope and could infringe on passengers' privacy. Others were concerned that the government should not rely on potentially flawed commercial data to prevent individuals from traveling by air. Some asserted that the use of knowledge discovery technologies on a wide variety of personal data could pose privacy and civil liberty violations. Finally, many wondered if individuals would be able to challenge their score.

In August 2003, TSA made available an Interim Final Privacy Notice on CAPPS II, which included substantial modifications to the initial proposal based on many of the concerns voiced in response to the first Privacy Notice.[5]

Under the Interim Notice, TSA would not keep any significant amount of information after the completion of a passenger's itinerary. Furthermore, TSA promised to delete all records of travel for U.S. citizens and lawful permanent residents a certain number of days after the safe completion of the passenger's travels (7 days is the current anticipation). TSA also committed to developing a mechanism by which a passenger targeted for more thorough screening can seek to set the record straight if they think they have been identified in error.

More importantly, the CAPPS II system addressed privacy concerns by severely limiting the types of private information collected and the way in which commercial data will be examined. The proposed CAPPS II system would have accessed only a "passenger name record" (PNR), which includes information collected at the time the passenger makes the reservations, prior to the flight. Selected PNR information (including name, address, date of birth, and telephone number) was to be transmitted to commercial data providers for the sole purpose of authenticating the passenger's identity. This process would be similar to the credit card application procedure used to check for fraudulent information.

Secure Flight—In 2004, TSA again modified its pre-screening program, now renaming it Secure Flight. According to a Privacy Impact Assessment and Systems of Records Notice published in September 2004, the principal difference between Secure Flight and CAPPS II was to further tighten the privacy protections and to split into two distinct pieces the operational components of the system.[6] One part of the system would match PNR data to existing Terrorist (and other "no-fly") watch lists. The second part would test whether the fidelity of PNR data (that is the clarity with which the data unambiguously identifies a single unique individual) could be enhanced through the use of commercial data bases.[7] Consistent with those notices, and with the Congressional mandate to do SO,[8] Secure Flight began a test of its system using historical data from June 2004 provided under order by the airlines.

The results of this testing have not yet been fully disclosed. In public remarks, however, TSA representatives have stated that the watch list matching portion of the project appears to have worked well, both in effectively matching PNR data with

---

[4] *See* 68 Fed. Reg. 2101 (Jan. 15,2003).

[5] *See* 68 Fed. Reg. 45265 (Aug. 1,2003).

[6] 69 Fed. Reg. 57345 (SORN, 57352) (PIA) (Sept. 24, 2004).

[7] A more detailed summary of the differences between CAPPS II and Secure Flight can be found in GAO, Secure Flight Development and Testing Under Way but Risks Should Be Managed as System is Further Developed, at Table 3 (GAO–05–356, March 2005).

[8] In the Intelligence Reform and Terrorism Prevention Act of 2004, Congress mandated testing of a passenger pre-screenig program. *See* IRTPA, Pub. L. No. 108–458, § 4012, 118 Stat. screening 3638,3714–19 (2004) (TSA directed to "commence testing of an advanced passenger prescreening system. . .utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government").

watch list information and in stress testing to demonstrate that the system is capable of handling the volume of inquires anticipated.

The best estimate is that after automated clearances, carriers operating independently have approximately a 2% "close" match rate—that is a rate that requires further inquiry and human intervention. This means that, on average there are 35,000 matches per day (assuming an average of 1.8 million travelers each day. Preliminary results suggest that with an "in-house" matching system run by TSA and with the addition of only the date of birth of an individual, this close match rate can be reduced by 60% to 0.8% of the travelling public—an average of 14,000 matches each day. If so, this will be a substantial improvement—and the use of commercial data has the potential to drive the number even lower, though testing is still ongoing.

Controversy has arisen regarding the program in the past few weeks, however, concerning its compliance with the original System of Records Notice (SORN) published in the Federal Register. The deviation was sufficiently great that TSA recently amended the notice of the scope of the system of records. In the original SORN[9] the system included only PNRs; information from the Terrorist Screening Center (TSC); authentication scores and codes from commercial data providers; and the results of comparisons between individuals identified in PNRs and the TSC watch list. The revised SORN,[10] issued last week, adds two new categories of information held in the system of records:

> PNRs that were enhanced with certain information obtained from commercial data—full name, address, date of birth, gender—and that were provided to TSA for purposes of testing the Secure Flight program; [and]

Commercial data purchased and held by a TSA contractor for purpose of comparing such data with June 2004 PNRs and testing the Secure Flght program.

The Privacy Officer has announced an investigation of Secure Flight to examine whether the actions which necessitated the modification of the SORN constituted a violation of Departmental privacy polices or law.

II. Secure Flight and Commercial Data

Why Secure Flight?—The Secure Flight program poses some interesting and challenging problems in adapting the law to new technology and the realities of new technology to the law. First, if Secure Flight is to be effective its hallmark will be the idea that some form of "result" will necessarily be immediately available to TSA screeners on a "real-time" basis so that they can make near-instantaneous decisions regarding whom to screen or not screen prior to allowing passengers to board the aircraft. If Secure Flight were designed so that detailed personal information on each passenger were transmitted to every TSA screener, all would agree that the architecture of the system did not adequately protect individual privacy. The analysis passed by the Secure Flight system to TSA employees at the airport must be (and under current testing plans, will be) limited to a reported color code—red, yellow or green—and should not generally identify the basis for the assignment of the code.

Thus, Secure Flight proposes to precisely reverse the privacy protection equation being developed in other contexts. To protect privacy, other information technology program disaggregate analysis from identity by making the data available to the analyst while concealing the identity of the subject of the inquiry unless and until disclosure is warranted. In the reverse of this paradigm, Secure Flight will disclose the identity of the potential threat (through a red/yellow/green system displayed to the screener, warning of a particular individual) but will conceal from the screener the data underlying the analysis—at least until such tie as a determination is made that the two pieces of information should be combined. The privacy protection built into Secure Flight is therefore the mirror image of the more common system. It is by no means clear which method of protecting privacy is *ex ante* preferable—but it is clear that the two systems operate differently and if we are to have any sort of Secure Flight system at all, it can only have privacy protections of the second kind.

Nor is Secure Flight necessarily a decrease in privacy. Rather, it requires tradeoffs in different types of privacy. It substitutes one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports). It will allow us to target screening resources, while actually *reducing* the number of intrusive searches: Currently 14% of the traveling public are subject to some form of secondary screening. Secure Flight may reduce that to as low as 4% selected for additional screening.[11] More importantly, Secure Flight will also have

---

[9] 69 Fed. Reg. 57345 (Sept. 24, 2004).

[10] 70 Fed. Reg. 36319 (June 22, 2005).

[11] *See* Transcript of Media Roundtable with DHS Under Secretary Asa Hutchison (Feb. 12, 2004) (available at *www.tsa.gov*).

the salutary effect of reducing the need for random searches and eliminate the temptation for screeners to use objectionable characteristics of race, religion, or national origin as a proxy for threat indicators.[12] For many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy, fewer random searches, and a reduction in invidious racial profiling.

Finally, and perhaps most saliently, Secure Flight is a useful idea because it will allow us to focus scarce resources. One of the truly significant improvements in homeland security has come from the use of risk assessment and risk management techniques to identify salient threats and vulnerabilties and target resources (like inspectors) at those situations where the threats and vulnerability are greatest. Thus, rather than attempt fruitlessly to search every container entering the United States, we use information about the shipper, place of origin and other factors to select for inspection containers about which there is some ambiguity or concern. So, too, with Secure Flight—we can envision the day when TSA inspectors (and other resources such as Air Marshals), are allocated in the way we think best addresses actual risks of harm, increasing the chances of catching terrorists and minimizing the unnecessary intrusion into people's lives at times and places where there is no risk at all. Should Congress have any concerns at all about the intrusiveness of individual screening it should, at a minimum, recognize the utility of enhanced risk assessment technology.[13] To fail to do so would be even worse than our current system.

Which brings us to the final question of effectiveness. Of course, before full deployment, Secure Flight needs to demonstrate that it can work. It holds great promise—but promise is far different from reality. Thus, the ultimate efficacy of the technology developed is a vital antecedent question. If the technology proves not to work-if, for example, it produces 95 percent false positives in a test environment-than all questions of implementation may be moot. For no one favors deploying a new technology—especially one that impinges on liberty—if it is ineffective. Thus, Congress is right to insist that Secure Flight be thoroughly tested. Conversely, we are unwise to reject it before knowing whether the effectiveness problem can be solved.

Some critics are skeptical that Secure can ever work, characterizing it as the search Bayesian probability problems.[14] That broad statistical criticism is rejected by researchers in the field who believe that because of the high correlation of data variables that are indicative of terrorist activity, a sufficient for a "silver bullet" that cannot function because of number of variables can be used in any model to create relational inferences and substantially reduce the incidence of false positives.[15] And, in other environments, enhanced technology allowing the correlation of disparate databases and information has proven to have potentially significant positive uses. American troops in Iraq, for example, use the same sorts of link and pattern analysis, prediction algorithms and enhanced database technology that would form a part of Secure Flight to successfully track the guerrilla insurgency.[16]

---

[12] Some purely random searches will need to be retained in order to maintain the integrity of the inspection system and defeat so-called "Carnival Booth" attacks (named after a student algorithm proposing a method of defeating CAPPS). Adding a random factor to the inspection regime answers the problem. *See* Samidh Chakrabati & Aaron Strauss, "Carnival Booth: An Algorithm for Defeating the Computer-assisted Passenger Screening," (available at *http://www.swiss.ai.mit.edu/6805/student-papers/sprig02-papers/caps.htm*) (describing program); KA. Taipale, "Data Mining and Domestic Security," 5 COOLUM. SCI. & TECH. L. REV. 2, AT N.285 (2003) (EXPLAINING HOW ADDITION OF RANDOM SCREENING GUARDS AGAINST SUCH ATTACKS).

[13] Risk assessment need not be used only to identify particular individual activity. We could also imagine a world in which Secure Flight were used only to identify resource allocation methods—surging TSA resources, for example, to at-risk flghts or airports without particularly singling out an individual for distinct scrutiny.

[14] *E.g.* Jeffrey Rosen, The Naked Crowd 105–06 (Random House 2004).

[15] *See* Remarks, David Jensen, "Data Mining in the Private Sector," Center for Strategic and International Studies, July 23,2003; David Jensen, Matthew Rattigan, Hannah Blau, "Information Awareness: A Prospective Technical Assessment," SIGKDD '03 (Augst 2003) (ACM 1–58113–737–0/03/0008).

[16] *See* AP, "Computer-sleuthing aids troops in Iraq," (Dec. 23,2003). Any who doubt that, in some form, enhanced information search technology can work need only contemplate the recent arrest of LaShawn Pettus-Brown, whose date identified hi as a fugitive when she "Googled" him. *See* Dan Horn, "Fugitive Done in by Savvy Date and Google," USA Today (Jan. 29,2004) (available at *http://www.usatoday.com/tech/news/2004–01–29-google-bustx.htm). Compare that with the pre-September 11 prohibition (eliminated by the new FBI guidelines) on the FBI's use of Google. See* L. Gordon Crovitz, "Info@FBIgov," Wall St. J. (June 5, 2002). At some fundamental level the ultimate question is how to reconcile readily available technology in commercial and

Continued

It is also important to realize that there may be potentially divergent definitions of "effectiveness." Such a definition requires *both* an evaluation of the consequences of a false positive and an evaluation of the consequences of failing to implement the technology. If the consequences of a false positive are relatively modest (e.g. enhanced screening), and if the mechanisms to correct false positives are robust (as recommended below), then we might accept a higher false positive rate precisely because the consequences of failing to use Secure Flight technology (if it proves effective) could be so catastrophic. In other words, we might accept 1,000 false positives if the only consequence is heightened surveillance and the benefit gained is a 50 percent chance of preventing the next terrorist flight attack. The vital research question, as yet unanswered, is the actual utility of the system and the precise probabilities of its error rates.[17]

Commercial Data—One part of the efficacy answer lies in the question of the use of commercial data to disambiguate and resolve identities. Clearly, it is plausible to believe that the incidence of false positives can be reduced by the use of commercial data. Credit granting institutions do it all the time. Thus, in theory, there ought to be no reason why reliance on commercial data to enhance efficacy should be ruled out of bounds.

Indeed, if using commercial data works to reduce the unnecessary screening of correctly identified individuals it will have the salutary effect of enhancing privacy. We need, of course, to test this aspect of Secure Flight as well to insure that it works, but if it does and if it can be implemented in privacy-protective ways, then identity verification should be welcomed, not opposed

The question then, is whether it can be done in a manner that is sufficiently privacy protective. The outlines for such a privacy-protective system can be seen in the original SORN issued for the Secure Flight testing phase. Most notably, that SORN limited the Secure Flight system of records to authentication scores and codes provided by commercial data providers—in other words, the actual data that forms the basis for the authentication score would remain with the commercial database and not be transmitted to TSA.

In my judgment, that system architecture strikes the right balance. It allows Secure Flight to take advantage of the commercial authentication methodology while minimizing the risk of governmental misuse of commercial data. It should be the cornerstone of a broader oversight structure to guard against abuse, which would include additional components along the following lines:

Though the details would need, of course, to be further developed, the outline of such an oversight system might include some or all of the following components:

- Secure Flight should be constructed to include an audit trail so that its use and/ or abuse can be reviewed;
- It should not be expanded beyond its current use in identifying suspected terrorists and threats to national security—it should not be used as a means, for example, of identifying drug couriers or deadbeat dads;[18]
- The program should sunset after a fixed period of time, thereby ensuring adequate Congressional review;
- Secure Flight authorization should have significant civil and criminal penalties for abuse;
- The "algorithms" used to screen for potential danger must, necessarily, be maintained in secret, as their disclosure would frustrate the purpose of Secure Flight. They must, however, also be subject to appropriate congressional scrutiny in a classified setting and, if necessary, independent (possibly classified) technical scrutiny;
- As outlined below, there must be an adequate redress procedure in place;
- Because commercial databases may contain errors, no American should be totally denied a right to travel (i.e. red-carded) and subject to likely arrest as a suspected terrorist solely on the basis of public, commercial data. An indication of ambiguous identification and lack of authentication should form the basis only for enhanced screening. Adverse consequences of arrest or detention should only be based on intelligence from non-commercial sources.

---

public use, with the broad governmental monopoly on the authorized use of force. Whatever the proper resolution, we cannot achieve it by hiding our heads in the sand and pretending that data integration technology does not exist.

[17]One final note—though privacy advocates are concerned about the false positives, the existence of an available system also may create civil tort liability for the failure to deploy. It is not fanciful to imagine tort suits against airlines that either do not implement Secure Flight or refuse to cooperate with TSA if by doing so they give rise to a false negative.

[18]*Cf.* William Stutz, "Local Policing After the Terror," 111 Yale L. J. 2137, 2183–84 (2002) (use of expanded surveillance authority to prosecute only terrorists and other serious offenses).

- The No-Fly/Red Card designation, though initially made as the product of a computer algorithm, should never transmitted to the "retail" TSA screening system until it has been reviewed and approved by an official of sufficiently high authority within TSA to insure accountability for the system.[19]

In my view, the recent controversy over commercial data provides an important lens through which to view the Secure Flight program. Evidently (though, of course, the facts are not yet known) TSA needed to enhance PNR data with commercial data in order to resolve residual identification ambiguities. This suggests, albeit indirectly, that the thesis of Secure Flight—that PNR data alone is sufficient to allow it to function—may be untenable. For the enhanced PNRs would probably not have been sought had they not been necessary. It also raises the question of whether the system's chosen architecture is the best—or whether in light of the necessity for enhancing PNRs we might not prefer a decentralized system.

But those questions are relatively technical in nature and, it seems, capable of resolution. The most significant aspect of the recent controversy is one of public perception. To that I now turn.

III. Compliance and the Privacy Act

Most Americans recognize the need for enhanced aviation security. They are even willing to accept certain governmental intrusions as a necessary response to the new threats.

But what they insist upon—and rightly so—is the development of systemic checks and balances to ensure that new authorities and powers given the government are not abused. And to achieve a suitable system of oversight, we need adequate transparency. We do not seek transparency of government functions for its own sake. Without need, transparency is little more than voyeurism. Rather, its ground is oversight—it enables us to limit the executive exercise of authority. Paradoxically, however, it also allows us to empower the executive; if we enhance transparency appropriately, we can also comfortably expand governmental authority, confident that our review of the use of that authority can prevent abuse. While accommodating the necessity of granting greater authority to the Executive branch, we must also demand that the executive accept greater review of its activities.

In that spirit, the Privacy Impact Assessments and Systems of Records Notices published by institutional actors like TSA serve several important functions. They define the program, they provide the opportunity for notice and comment on the program by the public and, most significantly, they provide a metric against which to measure the program's implementation. Prior notice of governmental activity is the hallmark of accountability—it fixes in time and place the ground for decision making and prevents *ex post* justifications from being developed.

Thus, we should be at least somewhat concerned by the recent revision of Secure Flights notice regarding the system of records being maintained. As I said earlier, the original SORN developed the right theoretical methodology for accessing commercial data for identify verification—maintaining the data in private hands and reporting the government only an authentication score. The most notable change identified in the new SORN issued last week is the breakdown in this screening methodology paradigm. To be sure, that change may prove to be a technical necessity—but if so, it is a change that ought to be publicly disclosed and debated before it is made. The fundamental premise of my analysis of Secure Flight (and indeed the analysis of all supporters and opponents) is that what is described in the TSA's privacy act notices is an accurate description of what is planned and what has happened. It undermines the transparency of the program and public confidence when that premise is proven wrong.

IV. Redress

Finally, the subject matter of the Secure Flight system calls for heightened sensitivity to the potential for an infringement on protected constitutional liberties. While Secure Flight will not directly affect personal physical liberty which lies at the core of constitutional protections, it does implicate at least one fundamental liberty, interest guaranteed by the Constitution. Since the 1960s the Supreme Court has recognized a fundamental right to travel[20]—indeed, one might reasonably say that one purpose of the Federal union was to insure the freedom of commerce and travel within the United States.

Thus, there is a risk that a poorly designed system will unreasonably impinge upon a liberty. The risk of such impingement should not result in fundamental con-

---

[19] This would mirror the view of the European Union which styles it as a "right" to have human checking of adverse automated decisions. The EU Directives may be found at *http://www.dataprivacy.ie/6aii–2.htm#15.*

[20] *Shapiro v. Thompson,* 398 U.S. 618 (1969).

stitutional abandonment of the program—especially not in light of the potentially disastrous consequences of Type II error if there is another terrorist attack in the United States. However, we will need stringent oversight to provide the requisite safeguards for minimizing infringements of civil liberty in the first instance and correcting them as expeditiously as possible.

Any appropriate redress mechanism will need to solve two inter-related yet distinct problems. *First,* it will need to accurately and effectively identify false positives without creating false negatives in the process. For though we know that any watch list system will make mistakes by wrongly singling out an individual for adverse consequences, we also know that a watch list system may err by failing to correctly identify those against whom adverse consequences are warranted. And we also know that any redress mechanism must be as tamper-proof and spoof-proof as possible, for it is likely that those who are correctly placed on a terrorist watch list will use any redress process available to falsely establish that they should not be subject to enhanced scrutiny.

Second, any redress mechanism must effectively implement the requisite corrective measures. Already we have seen situations in which acknowledged "wrongly matched" errors in watch list systems cannot be readily corrected because of the technologically unwieldy nature of the information systems at issue. Even when TSA has recognized that a given person (for example, Senator Edward Kennedy) is repeatedly wrongly matched to a "no fly" list entry, correction proves challenging as one cannot just remove the more ambiguous watch list entry.[21] Thus, the legal, policy, and technological mechanisms must be built in to the watch listing system to allow for the effective handling of redress.

Sadly, the limitations of this forum prevent me from providing you a detailed of exactly what a system answering these questions would look like. But my colleague Jeff Jonas and I have written in detail about this question.[22] In short, we envision a system of third-party ombudsman-like review; initial administrative review; limitations on disclosure if necessary to accommodate national security concerns; a private cause of action to correct any permanent deprivation of liberty; and a system design requirement tethering and attributing information so that corrections propagate through the system rapidly. Our conclusion is that these questions are soluble—and that prior to full-scale implementation TSA must solve them.

In short, Secure Flight continues to have some significant issues that need to be addressed. But it also is a system of great promise. Failing to make the effort to use new technology wisely poses grave risks and is an irresponsible abdication of responsibility.

As six former top-rankig professionals in America's security services recently observed, we face two problems-both a need for better analysis and, more critically, "improved espionage, to provide the essential missing intelligence." In their view, while there was "certainly a lack of dot-connecting before September 11," the more critical failure was that "[t]here were too few useful dots."[23] Secure Flight technology can help to answer both of these needs. Indeed, resistance to new technology poses practical dangers. As the Congressional Joint Inquiry into the events of September 11 pointed out in noting systemic failures that played a role in the inability to prevent the terrorist attacks:

> 4. Finding: While technology remains one of this nation's greatest advantages, it has not been fully and most effectively applied in support of U.S. counterterrorism efforts. Persistent problems in this area included a lack of collaboration between Intelligence Community agencies [and] *a reluctance to develop and implement new technical capabilities aggressively. . . .*[24]

---

[21] *See* Sara Goo, "Sen. Kennedy Flagged by No-Fly List," *The Washington Post,* August 20, 2004, p. A1. Others on the list, like Representative John Lewis, avoided secondary screening by including their middle initial. *See* Jeffrey McMurray, "Rep. Lewis says his name is on terrorist watch list," Associated Press, August 20, 2004.

[22] *See* Rosenzweig & Jonas, Correcting False Positives: Redress and the Watch List Conundrum, Legal Memorandum No. 17 (The Heritage Foundation, June 2005) (avaiable at *http://www.heritage.org/Research/HomelandDefense/lm17.cfm*)

[23] Robert Bryant, John Hamre, John Lawn, John MacGaffin, Howard Shapiro & Jeffrey Smith, "America Needs More Spies," *The Economist,* July 12, 2003, p. 30.

[24] *Report of the joint Inquiry Into the Terrorist Attacks of September 11, 2001, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rept. No. 107–351 and H. Rept. No. 107–792, Dec. 2002, p. xvi (available at http://wwwjas.org/irp/congress/2002&—rpt/911 rept.p4f (emphasis supplied). The Joint Inquiry also critiqued the lack of adequate analytcal tools, id.* Findings 5, and the lack of a single means of coordinatig disparate counterterrorism databases, *id.* Findigs 9 & 10. Again, aspects of the CAPPS II program are intended to address these inadequacies and litations on the research program are inconsistent with the Joint Inquiry's findigs.

Or, as one commentator has noted, the reflexive opposition to speculative research by some is "downright un-American."[25] Though Secure Flight technology might prove unavailing, the only certainty at this point is that no one knows. It would be particularly unfortunate if Congress opposed basic research without recognizing that in doing so it was demonstrating a "lack [of] the essential American wilingness to take risks, to propose outlandish ideas and, on occasion, to fail."[26] That flaw is the way to stifle bold and creative ideas—a "play it safe" mindset that, in the end, is a disservice to American interests.

Mr. Chairan, thank you for the opportunity to testify before the Subcommittee. I look forward to answering any questions you might have.

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

The Chair would now recognize Mr. James Dempsey, the executive director of the Center for Democracy and Technology, for his testimony.

STATEMENT OF JAMES DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DEMPSEY. Chairman Lungren, Chairman Cox, Mr. Thompson, members of the subcommittee, good morning. Thank you for the opportunity to testify today.

Let me start, Mr. Chairman, with two basic points. First of all, in my view, we need a passenger pre-screening system. Passenger airlines remain a target of terrorists. Every day, 1.5 to 1.8 million passengers board airplanes in the United States for domestic flights. It is infeasible to intensively scrutinize each of those passengers. To focus resources, it is necessary to make judgments about them before they reach the security checkpoint. Therefore, one element of the layered security system for air transport should be the pre-screening of passengers.

Second, in developing a passenger screening system, privacy is not a luxury. By privacy, I really mean fair information practices. How much information is collected? Is it accurate? How is it used? With whom is it shared? How long is it kept? Answering these privacy questions is not a distraction from the task of preventing terrorist attacks.

To the contrary, addressing these information collection and use issues is part of the process for designing an effective system, from a security standpoint, as well as from a privacy and public trust standpoint, because as Mr. Rosenzweig said, every minute airport screeners spend inconveniencing an innocent person is an opportunity for the terrorist to slip by undetected.

Here is how I would do it. First, I would preserve the CAPPS I behavioral rules. I have changed my own opinion on this. I now no longer believe that CAPPS I is broken. CAPPS I, after all, correctly flagged 9 of the 19 September 11 hijackers. At the time, that only meant that their luggage had to be checked and the individuals themselves were not subject to more scrutiny. But the behavioral rules of CAPPS, even though to some extent they have been publicly discussed, are flexible, they are useful enough and they should be continued.

Moreover, I believe that CAPPS rules should continue to be administered by the airlines. While Section 4012 of the Intel Reform Act requires the government to bring in-house the process of

[25] *See* David Ignatius, "Back in the Safe Zone," *The Washington Post,* August 1, 2003, p. A19.
[26] *Id.*

matching passenger data with watch lists, TSA seemed to be suggesting in its latest Secure Flight notice that it might also assume full responsibility for administering the behavioral rules of CAPPS. If so, that would be a big change with major implications for privacy since the application of CAPPS rules require a lot more data, even more data than is in the passenger name record, and I just do not see either technically or from a public policy standpoint how the government could possibly take in that kind of data. So leave that with the airlines.

Second, put on top of it the screening of passengers against the watch list, and that should be done by the government, not the airlines. That is what the 9/11 Commission recommended, and that is what Congress mandated last December in the Intel Reform Act.

We have many data quality issues to resolve with those watch list and with the matching process, but if we have that list of suspected terrorists, we should use it to decide who deserves closer scrutiny.

In my view, however, the passenger name record is not a good source of information for matching. It does not have what is needed, full name and date of birth, and it has too much irrelevant information. I believe, currently, in my view, the airlines should be required to collect and provide to the government or only what is necessary to make a reliable match.

The problem with watch list matching is that the categories of information in the watch list do not match the categories of information in the PNR record, the passenger name record. So you are trying to match apples and oranges, and name alone of course is worse than worthless; it is harmful trying to match on name alone because you get far too many hits.

So now the third question and the possible third element of a passenger pre-screening system is the use of commercial data. It may be useful, but so far we have not seen the evidence. I do wonder why TSA has been looking at using commercial data to augment PNR on millions of passengers a day when I think there may be better value from using commercial data at the TSC to augment the watch list data on the 200,000 or so people in the watch list to try to figure out can we figure out better identifying information on them.

There is a lot of commendable work that TSA has done, and we clearly rely upon the screeners for our safety, and they have an extremely difficult job. TSA stumbled badly when its testing procedures departed from its privacy notices, but we must not let this controversy detract from the more important issues that remain, still unanswered, about how Secure Flight will work.

It is on those questions of data collection and use that this committee and TSA and my organization should focus.

I am committed to working with you, Mr. Chairman, and this subcommittee as well as with TSA to resolve those questions to develop a more effective passenger screening system.

Thank you.

[The statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Chairman Lungren, Ranking Member Sanchez, Members of the Subcommittee, thank you for the opportunity to testify today.

I am Executive Director of the Center for Democracy and Technology. CDT is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the digital age. I am also privileged to serve as an associate member of the Markle Foundation Task Force on National Security in the Information Age. The Markle Task Force, co-chaired by Zoë Baird and Jim Barksdale, is comprised of leading experts from the fields of national security, technology, and privacy, including CDT's President Jerry Berman. Its members have extensive experience in and out of government at the federal and state level, in both the legislative and executive branches, from the administrations of Presidents Carter, Reagan, George H.W. Bush, Clinton, and George W. Bush. The Task Force has published two reports, "Protecting America's Freedom in the Information Age" (2002) and "Creating a Trusted Information Network for Homeland Security" (2003), available at *http://www.markletaskforce.org.* The Task Force, which is continuing its work, has offered concrete recommendations for strengthening national security while protecting civil liberties by creating a decentralized network for sharing and analyzing information within a framework of accountability and oversight. This testimony is based in large part on recommendations the Task Force submitted to the Transportation Security Administration in February of this year.

I. Background and Summary of Conclusions

Terrorists continue to target passenger airplanes. One element of a layered security system for air transport is the screening of passengers. Every day, over 1.5 million passengers board airplanes in the United States for domestic flights. It is infeasible to intensively scrutinize each of those passengers. To focus resources, it is necessary to make judgments about passengers before they reach the security checkpoint.

The Transportation Security Administration (TSA) is testing a proposed passenger screening system named Secure Flight. The system is mandated by Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108–458). It would implement a recommendation of the 9/11 Commission.

Section 4012 of the Intelligence Reform Act requires TSA to "assume the performance of the passenger screening function of comparing passenger information to the automatic selectee and no fly lists and utilize all appropriate records in the consolidated and integrated terrorist watch list maintained by the Federal Government in performing that function." Section 4012 specifies that DHS must:

- include a procedure to enable airline passengers who are delayed or prohibited from boarding a flight because of the system to appeal such determination and correct information in the system;
- ensure that databases that will be used to establish identity of passengers will not produce a large number of false positives;
- establish an internal oversight board;
- establish sufficient operational safeguards to reduce the opportunities for abuse;
- implement substantial security measures to protect against unauthorized access;
- adopt policies establishing effective oversight of the use and operation of the system; and
- ensure that there are no specific privacy concerns with the technological architecture of the system.

Section 4012 also requires the Secretary of Homeland Security, in consultation with the Terrorist Screening Center, to "design and review, as necessary, guidelines, policies, and operating procedures for the collection, removal, and updating of data maintained, or to be maintained, in the no fly and automatic selectee lists."

In addition, section 522 of the fiscal year 2005 DHS Appropriations Act (Pub. L. No. 108–334), required the Government Accountability Office to assess 10 aspects of Secure Flight development and report to Congress, which GAO did in March of this year."[1]

On September 24, 2004, even before the Intelligence Reform Act was adopted, but after the report of the 9/11 Commission was widely endorsed, the TSA released three documents that outlined plans for testing Secure Flight. As detailed in a Privacy Act Notice, Privacy Impact Assessment, and Emergency Clearance Request

[1] U.S. Government Accountability Office, "Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed," March 2005, GAO–059–356.

(collectively, the "September 2004 Notices"),[2] Secure Flight would have three components:

- collection from the airlines of identifying information contained in the Passenger Name Records (PNRs) for matching against the consolidated watch list of the FBI's Terrorism Screening Center (TSC);
- possible use of commercial databases of personally identifiable information to verify the information provided in the PNR; and
- use of "streamlined" behavior rules drawn from the current Computer Assisted Passenger Prescreening System (CAPPS I), which uses behavioral factors such as purchase of a one-way ticket to select passengers for enhanced scrutiny.

While use of commercial data and continued use of CAPPS I rules were not required in Section 4012, they have remained part of the Secure Flight plan and test. Moreover, in regards to the use of commercial data, it is now clear that TSA is examining not merely its value to verify identity but also its value in augmenting PNR information to make a better watch list match. Furthermore, while Section 4012 requires the government to bring "in-house" the process of matching passenger data with watch lists, TSA seems to be saying in its latest Secure Flight notice that it will also assume full responsibility for administering the behavioral rules of CAPPS. If so, this is a big change, with major implications for privacy, since application of the CAPPS behavioral rules would require the government to access much more personal information than required for watch list matching.

To test Secure Flight, TSA required airlines to turn over all Passenger Name Records (PNRs) from June 2004. TSA has been using this historical data to test the efficacy of its proposed system, including the possible use of commercial data, and to compare results under Secure Flight with results under the old CAPPS system. In general, passengers face no adverse consequences in the test phase, unless the search turns up a name on the watch list as having been on a flight last June, in which case the FBI will be notified. According to TSA, no such notification has been justified.

There are several commendable elements of TSA's process in developing Secure Flight:

- In response to congressional oversight and public criticism, TSA fundamentally re-examined the previous proposal for a new airline passenger security program, the second-generation Computer Assisted Passenger Prescreening System ("CAPPS II").
- After issuing an opaque Privacy Act notice on CAPPS II in January 2003, TSA took a more transparent approach, with both the CAPPS II notice of August 2003 and the Secure Flight notices of September 2004. This included the publication of a Secure Flight Privacy Impact Assessment (PIA) *before* going forward with the test phase, an important precedent within DHS and for other agencies.
- Before implementing a new passenger screening system, TSA is conducting testing to determine what is most effective. From the September 2004 Notices, it would appear that TSA has not prejudged the outcome of the testing.
- In its Secure Flight proposal, TSA appears to have dropped some of the most troublesome aspects of CAPPS II, including the probability-based review of all passengers based on unidentified government data to determine each passenger's "risk" score and the notion of using Secure Flight for purposes other than enhancing the security of domestic flights by identifying passengers who warrant further scrutiny prior to boarding an aircraft based on possible terrorist connections.

However, TSA stumbled badly when its testing procedures departed from the assurances it provided to Congress and the public in the September 2004 Notices. In particular, contrary to indications in the Notices, TSA and its contractors acquired and retained personal information from commercial databases, as TSA admitted in a revised notice issued earlier this month.[3] This misstep has once again cast doubt on the credibility of the government.

However, we must not let this controversy detract attention from much more important issues that remain unanswered about Secure Flight. Important efficacy, privacy and due process issues remain to be resolved before full implementation can begin. As the GAO found in its March 2005 report:

---

[2] Notice to Establish System of Records, Docket No. TSA–2004–19160, 69 Fed. Reg. 57345 (Sept. 24, 2004); Notice of Privacy Impact Assessment, Docket No. TSA–2004–19160, 69 Fed. Reg. 57352 (Sept. 24, 2004); Notice of Emergency Clearance Request, Docket No. TSA–2004–19160, 69 Fed. Reg. 57342 (Sept. 24, 2004).

[3] Notice to Supplement and Amend Existing System of Records and Privacy Impact Assessment, Docket No. TSA–2004–19166, —— Fed. Reg. ———(June 20, 2005).

- "the effectiveness of Secure Flight in identifying passengers who should undergo additional security scrutiny has not yet been determined" (p. 27);
- "the accuracy of commercial data is uncertain" (p. 32);
- "key issues regarding how [PNR] data will be obtained and transmitted have not yet been resolved" (p. 29);
- "the ability of Secure Flight to make accurate matches between passenger data and data contained in the terrorist screening database is dependent on the quality of the data [in the screening database]. . . .the accuracy of this data has not been fully determined" (p. 6).

In particular, because expanded watch lists are the core of the proposed program, the fidelity, data quality and overall reliability of those watch lists will be very important. In June of this year, the Department of Justice Inspector General found that the Terrorist Screening Center could not ensure that the information in the watch list database was complete and accurate. The IG's report identifies a number of types of errors in TSC data.[4] While TSA has begun to develop its own redress procedures, it should work with other agencies to develop standards for watch listing and redress mechanisms so passengers will have the ability to challenge a watch list entry or an erroneous watch list match. Proper resolution of those issues will be critical to the success of any air passenger screening system, in terms of both enhanced security and protection of civil liberties. The Intelligence Reform Act required the Executive branch to develop criteria and minimum standards for watch listing. As far as we know, those criteria and standards have not been developed.

Moreover, the controversy over collection of commercial data in the test phase of Secure Flight must not obscure more important questions: Where are the results of the test of matching June 2004 PNR data against the watch list and how will the lessons learned from the test affect implementation of Secure Flight? What has TSA learned from its test of commercial data, and what does it intend to do with commercial data if Secure Flight is permanently implemented? What has TSA determined is the best method for matching names? What is the quality of PNR data and what is the best way for the government to get the minimum amount of data to make reliable matches? These and other key questions should be the focus of Congressional and public oversight.

II. Watch Lists

TSA has accepted—and Congress has mandated—the recommendation of the 9/11 Commission that airline passengers should be screened against terrorist watch lists and the government, not the airlines, should perform that such screening. Secure Flight should be an improvement over the current CAPPS, because the watch lists should offer a particularity of suspicion that behavioral rules cannot, and because it is not desirable to disclose the watch list to airlines. Despite these advantages, however, Secure Flight will only be as good as the watch lists on which it is based and the way in which they are searched. The watch list to be used by TSA is a subset of the consolidated watch list (known as the Terrorist Screening Database (TSDB)) managed by the FBI's Terrorist Screening Center (TSC).

Watch list fidelity and data quality are critical to Secure Flight's success. "Fidelity" speaks to the robustness of entries: Do they contain enough information to resolve identity? "Data quality" refers to the accuracy, completeness and currency of the data. Related questions include: Are entries reviewed periodically for data quality? Has there been an evaluation of the reliability of criteria for designating individuals to the TSC watch list?

There should be a focus across the intelligence community on improving the quality of watch list entries. We appreciate that TSA does not create terrorist watch lists, but rather is a consumer of them. Nonetheless, Secure Flight will be the first time that the TSDB is used regularly to screen a significant portion of the U.S. public, and TSA will receive the brunt of the criticism if the watch list produces a significant number of false positives. Accordingly, TSA should play a lead role in developing and refining watch list standards.

Thus far, it is not clear whether there are adequate rules for watch list entries. While we understand the national security concerns associated with making public certain information about watch lists, we believe that, considering the critical importance of the watch listing process, the process and accountability measures associated with it should be publicly discussed.

Section 4012(c) of the Intelligence Reform Act requires the Director of National Intelligence, in consultation with the Secretary of Homeland Security, the Attorney General and the Secretary of State, to report to Congress in June 2005 on the cri-

[4] U.S. Department of Justice, Inspector General, "Review of the Terrorist Screening Center," June 2005, Audit Report 05–27, at p. xi.

teria for placing names on the watch list, the minimum standards for reliability and accuracy of identifying information, the degree of information certainty and the range of threat levels to be associated with an individual on the watch list, and the range of consequences that are to apply to an individual, if located. As far as we know, that report has not been submitted.

It is clearly preferable that watch listing standards be government-wide. In the absence of government-wide standards, TSA has adopted its own internal standards as to what constitutes an "adequate" watch list entry for purposes of Secure Flight. Such standards might include requirements like:

- There should be minimum fidelity standards before a watch list entry can be used. Each watch list entry used by TSA should contain enough identifying information so that the record can meaningfully be used for its intended purpose of identifying an individual. For example, TSA may require multiple data points, such as a first and last name as well as another piece of identifying information, such as date of birth. Name plus nationality or name plus gender is not enough.
- Each watch list entry used by TSA should be reviewed at least once a year by the agency that was responsible for its nomination to the list, to ensure that that the record still meets watch listing criteria and fidelity and data quality standards.
- To promote data quality and redress, each watch list entry should be traceable to a specific transaction (i.e., record) within the source agency, using an internal reference number or some other means of "tethering" the data, so that questions can be resolved and source system records can be reconciled with watch listing system records.

In addition, the use of any watch list for screening purposes depends on reliable match criteria. TSA should establish reliable matching criteria and should periodically reevaluate them.

Finally, as indicated in Section 4012(c) of the Intelligence Reform Act, another aspect of watch listing concerns the seriousness of the threat posed by a watch-listed individual and the different types of consequences that a person may face as a result of being placed on a watch list. An individual on a watch list should face consequences appropriate to the threat that individual is believed to pose. More than 200,000 people are listed in the TSDB—ranging from those known with certainty to be members of a terrorist organization to those suspected of having some tie to terrorism. The current situation is very confusing. Each of the international terrorist names included in the TSC database is assigned one of 25 different codes that describe how a specific individual is associated with international terrorism. Each of the domestic terrorist records is assigned one of three codes, which the DOJ IG concluded do not provide an adequate description. In addition, all entries are marked with one of four levels of "handling instructions," advising users what action to take when they encounter a watch listed person. On top of that, however, TSA draws a two-tiered distinction between "no fly" and "selectee." As a matter of policy, these distinctions and their basis need to be clarified.

III. Collection of Passenger Name Records

The Passenger Name Record (PNR) generated by airlines and reservation systems contains numerous pieces of information beyond the identifying information necessary to make a match for screening purposes, but, on the other hand, may not contain the data needed to make a reliable identification (e.g., the address and phone number on the PNR quite often is that of a travel agency, and date of birth is not included in the PNR). We understand that it would have been quite expensive for airlines to provide only certain PNR fields for the testing phase. Based, however, on the results of the test phase, TSA should determine exactly what data it needs to achieve the aviation security goal of Secure Flight. Then, if feasible, when Secure Flight is implemented permanently, TSA should collect from the airlines and reservations systems only those data elements that are necessary. One of the goals of the test phase should be to explore with the airlines and the reservations systems the feasibility of isolating and delivering to the government only those items of information for which the government has a justified need.

If TSA requires airlines to collect any additional information that they do not currently collect, such as date of birth, TSA should ensure that passengers are given notice about the reasons for the new collection of information. Alerting passengers to the purpose for which their information will be gathered—telling them that it is for security purposes as opposed to, say, marketing uses—should give law-abiding travelers an incentive to provide accurate information when booking air travel, enhancing privacy and effectiveness.

Also, if TSA requires airlines and reservation agents to collect information they do not currently collect, the airlines and other ticketing agents should be prohibited from retaining and using that data for any other purpose. While TSA has promised that it will not be compiling travel dossiers on passengers, neither should the travel industry be able to turn a TSA security order into an opportunity to compile new categories of information on air travelers for the airlines' or travel agents' own use.

TSA has announced that it intends to limit its retention of PNR data, but has not yet set specific retention periods. Once Secure Flight is implemented, TSA should not keep passenger data after a flight has safely completed its flight without incident, except that TSA may retain and disclose to the FBI and other relevant agencies the records of "reds" or no-flies who are not allowed to board and of "yellows" or selectees who are identified based on a watch list match but allowed to board after a more intensive search. Also, TSA should be able to retain data with the consent of any passenger who has invoked the redress process. These retentions and disclosures, which would have a sound predicate in the form of the match to the watch list, should be documented and auditable. Of necessity, given the verification process that should occur for every red and yellow, the TSC would receive (and should be able to retain) a record of the hit.

IV. Use of Commercial Data

Databases held by commercial entities contain a vast amount of data possibly relevant to screening activities, but they also pose challenges in terms of relevance and reliability. TSA and other policymakers, through a process with some transparency and outside input, need to make an assessment of what commercial data would be relevant to passenger screening. In the test phase, TSA has been exploring two potential uses of commercial data: (1) to augment PNR data with additional identifying information: and (2) to verify the identity of passengers. TSA should take a skeptical approach to the use of commercial data in the Secure Flight program, particularly regarding whether the identity scores provided by searching commercial data will significantly enhance TSA's certainty about passengers' identities.

If TSA decides to use commercial data in connection with Secure Flight, it should be on the basis of a finding that the use of commercial data would give additional certainty about the identities of a substantial number of passengers or a more reliable watch list match. Some questions to be considered during testing include:

- What minimum amount of information is required to even test a person for a true identity likelihood score using commercial databases?
- How many people, when providing true identifying information, fail to correlate with commercial databases? For example, what percentage of people flying to, from or within the United States will not have adequate information about them in commercial databases to do identity verification?
- How much reliability does the identity verification process add?
- Will identity verification work with individuals who have privacy concerns and use a different address (e.g., PO Box) than what appears on their driver's licenses, who legitimately have multiple addresses and phone numbers or whose addresses do not match because they use a different billing address for their credit cards?
- What consequences can flow from a poor "identity" score (as opposed to a watch list match)? Will a poor identity score in and of itself suggest a threat to aviation and trigger secondary inspection?

If TSA decides to use commercial data in Secure Flight, then a number of additional privacy protections will need to be implemented. First, TSA should clarify what passenger-provided information will be disclosed to commercial data aggregators. As explained above, passenger PNRs often provide sensitive and/or irrelevant information. TSA should not pass information on to commercial vendors without justification, and it should specify in advance which items of information it will be disclosing to the commercial aggregators.

Second, TSA should, to the maximum extent possible, specify what commercial information its vendors will rely on for the passenger identity verification process. TSA has made clear that neither it nor its commercial vendors will use credit scores, but it has been silent on what information they would rely on. While there are national security concerns at stake, it may be possible to reveal what *commercial* data is being used. One approach to these kinds of issues is to require the commercial data aggregators who are government contractors to make available for free upon request (maybe just once a year) all data they have on an individual for review and correction, the same way they are required to under the Fair Credit Reporting Act. This is in keeping with the commercial data aggregator's interest in having accurate information. Alternatively, the TSA could be required to use aggregators that can guarantee reconciliation accuracy with their data source providers. The trans-

parency into what is used would reveal sources such as public records, credit headers, phone books, driver's licenses, etc. In any case, the consumer should be able to request what information the TSA uses and its source, with instructions on how to remedy inaccuracies (at the source system). In this regard, providing travelers with notice and access to their data may increase the reliability and accuracy of the sources that TSA employs. TSA could include language in its contracts with commercial data vendors that provides for passenger access to and correction of that data directly or through the Passenger Advocate Office that TSA will establish.

Third, TSA should make clear that commercial vendors will, by contract, be prohibited from retaining any airline passenger data other than minimum amounts of data for audit and accountability controls or using it for any purpose other than testing for Secure Flight.

Finally, TSA should develop standards for assessing and verifying the accuracy of the commercial data on which it relies. TSA might base such standards on the answers to the following types of questions: (1) How often are the data updated? (2) How complete is the information? (3) How accurate is it? (4) How do the data sources protect against and/or mitigate the possibility of identity theft?

V. Redress and Oversight

Redress and oversight are important aspects of any decision making process based on personally identifiable information. As TSA implements Secure Flight, redress will be a major issue.

Major federal privacy laws offer sound models for Secure Flight redress procedures. As reflected in the Privacy Act, the Fair Credit Reporting Act, and other privacy laws, redress typically includes the following elements:

- Notice of the fact of an adverse decision and of the procedure for challenging it;
- Access to the information on which the decision is based;
- An opportunity to correct erroneous information and an obligation by the decision-maker to correct or delete information that is erroneous, which is premised on the ability to trace information to its source for verification;
- Procedures for ensuring that erroneous information does not re-enter the system;
- Obligations on data furnishers to respond to requests for reconsideration of data and to take corrective action when justified; and
- Independent administrative or judicial review and enforcement.

TSA has already committed to developing a "robust review and appeals process" to protect passengers' ability to seek redress where incorrect information or inferences cause them to be subjected to heightened scrutiny. As part of that process, TSA has indicated that it will create a Passenger Advocate Office, which will act on behalf of passengers and investigate complaints. The proposed Passenger Advocate is a desirable component of a passenger redress process, but TSA will need to flesh out the procedures that will govern the Passenger Advocate's review of passengers' complaints. It will be critical to the success of any new program that individuals have a meaningful process for challenging their "yellow" or "red" designations.

As noted above, we believe that TSA should not keep data on cleared passengers after a flight is successfully completed. For the relatively small number of passengers who may complain due to being selected for whatever reason, TSA should be able to preserve data if a passenger makes a complaint at the airport at the time of screening.

The Intelligence Reform Act requires TSA to establish a timely and fair process for individuals identified as a threat to appeal to TSA that determination and to correct any erroneous information. The process must include the establishment of a method by which TSA will be able to maintain a record of air passengers and other individuals who have been misidentified and have corrected erroneous information. To prevent repeated delays of misidentified passengers and other individuals, the TSA record shall contain information to authenticate the identity of such a passenger or individual.

Particularly in the context of individuals who appear to be a risk because of a watch list match, TSA must work closely with TSC to ensure that people are not mistakenly flagged on a repeat basis. As we already have seen, there will be innocent individuals with the same or similar names as people on the watch list. Such mistakes must be investigated and rectified quickly so that the affected individuals are not repeatedly flagged and delayed. This will require TSA to work closely with TSC and various intelligence agencies.

Passengers should have the ability to challenge the Passenger Advocate's decisions. First, passengers should be able to mount an administrative appeal within

TSA or the Department of Homeland Security, perhaps to the Privacy Officer. Second, given that the right to travel is at stake, judicial review should also be available once administrative appeals are exhausted. In some cases, judicial review might require special *ex parte* procedures to deal with classified information, but such procedures have been successfully implemented in other contexts. *See, e.g.,* Classified Information Procedures Act, Public Law 96–456.

In addition to redress, TSA should implement other oversight mechanisms. Auditing should be an important part of the Secure Flight system. The DHS Inspector General, the Privacy Officer, and the Civil Rights and Civil Liberties Officer should jointly conduct an annual audit of the system's operations. Of necessity, the auditors should have security clearances enabling them to access all relevant information, including classified data. The auditors could conduct spot checks of actual screenings and retain some passenger records for the duration of the audit process as well as examine the aggregator' datasets. To the extent an audit report relies on classified information, portions of the report may need to remain classified, but much of the audit reports could be made public.

TSA also should implement a real-time auditing function to monitor who accesses the system. TSA and TSC both must implement a documented information security program (to protect the data) and data governance models (to control access to the data and ensure access and modification are auditable). Such audit trials are crucial to prevent abuse and internal security breaches, ensuring that only authorized personnel are accessing the system and that they are using it only for authorized purposes.

Other forms of independent oversight of Secure Flight are also essential to an effective privacy protection scheme. TSA should report annually and publicly to Congress, including (1) an explanation of the Secure Flight privacy policies; (2) a description of how those policies have been implemented; (3) a list of the types of passenger complaints that have been filed, with descriptions of how they have been resolved; (4) changes that TSA is making to minimize any identified problems; and (5) the ratio of hits, no hits, and disposition results to allow evaluation of the false positive counts. Other oversight mechanisms that TSA should consider are independent evaluations of the program by outside auditors and periodic consultations with privacy advocates.

VI. Scope

Over the course of the evolution of CAPPS II and Secure Flight, there has been uncertainty about the mission that a passenger screening system should serve. In the spring of 2003, then-TSA Administrator Admiral James Loy assured Congress and the public that CAPPS II would be used only to identify foreign terrorists and prevent them from boarding airplanes, because foreign terrorists were the source of the threat to aviation security. Subsequently, TSA proposed broadening CAPPS II's purposes to include identification of domestic terrorists and those associated with domestic terrorist organizations as well as certain criminals and possibly immigration law violators.

In the September 2004 Notices and in the June 2005 Notice, TSA refocused on the threat of terrorism. The task of creating an effective system to screen passengers against terrorist watch lists is so urgent and so challenging that it is preferable at this point for TSA not to pursue the additional and separate task of identifying other criminals not believed to pose a threat to aviation.

Like CAPPS II, the proposal for Secure Flight includes not only foreign terrorists, but also members of domestic terrorist groups—i.e., members of radical organizations like the KKK, anti-government militias, or certain radical environmental activists. It might be sensible to include domestic terrorists in Secure Flight if there is evidence that particular individuals or discrete groups pose a threat to civil aviation. In the absence of intelligence suggesting that particular individuals or groups are a threat, the expansion of Secure Flight into the realm of domestic terrorism raises a host of difficult issues that TSA appears not to have confronted. It could ultimately place TSA in the role of having to evaluate the political activities of Americans. The FBI's definition of who is a domestic terrorist has often been quite broad. In the absence of a specific threat, does the term "domestic terrorist" include all members of a environmental group, when a few of those members that have engaged in illegal acts and have been investigated by the FBI as domestic terrorist organizations? Does it include an anti-abortion activist who breaks the law by blocking access to abortion clinics or who may be organizationally or ideologically related to those who have killed doctors or committed arson at clinics, which some have called terrorism? Does it include protesters against the war in Iraq, whom the FBI interviewed in advance of the Republican National Convention?

Furthermore, each added function puts further pressure on the system: more false positives, diversion of screener resources, loss of screener confidence in system results, and the risk of public disapproval. Accordingly, TSA should limit screening of passengers for associations with purely domestic terrorist organizations to those situations, if and when they arise, when information indicates that specific individuals or discrete groups pose a threat to civil aviation.

VII. Privacy Act

The Privacy Act offers a sound framework for a number of issues posed by Secure Flight. In the September 2004 Notices, TSA proposed exempting the Secure Flight test data from various Privacy Act provisions. Moreover, TSA had indicated that it would invoke blanket exemptions for full implementation of CAPPS II.

In the Notice issued last week, TSA announced that it would not pursue its Privacy Act exemptions. We commend this decision, and we urge that it be followed in the implementation of Secure Flight as well. TSA has always said that it plans to provide access to certain unclassified records such as PNR and the ability to correct them, as an important element of the integrity of the system. There seems to be, on the current record, no valid reason to take a exemption from the Privacy Act provisions on access and right to correct. If there are specific concerns that TSA has about application of the Privacy Act to Secure Flight in the implementation phase, it should identify them so they can be addressed based on a public dialogue.

Conclusion

We firmly believe that a passenger screening system can be designed that that both enhances security and protects civil liberties. Developing sound privacy rules and sticking to them is crucial to the success of such a program. To facilitate public trust in the system that is eventually implemented, we encourage TSA to make public as much as possible about the results of Secure Flight testing and TSA's decision-making process. We look forward to working with TSA and the Congress.

Mr. LUNGREN. Thank you very much, Mr. Dempsey.

I thank all the witnesses on this panel for their testimony.

At this time, I would yield myself 5 minutes to begin the questioning.

To Mr. May, Mr. Rosenzweig and Mr. Dempsey, there has been a suggestion that CAPPS I ought to remain as it is. There seems to be some divergence of opinion with the three of you, but I will just ask you this question: We have had situations where people have been taken out for a secondary search that obviously do not belong there, and I keep harkening back to children, instances of 10-year-olds, 5-year-olds, 3-year-olds, 2-year-olds being carried out.

Every time I have asked the question of TSA, the answer is, "That is the airline's responsibility. If they see someone is under 12 years of age, they are not supposed to take them out of the secondary search." But it does not happen. And then it goes to the TSA people and they say, "Well, since CAPPS I is not in our bailiwick, we cannot make that decision." Obviously when you see an infant in diapers, they are obviously under the 12.

That is my concern if you keep the CAPPS Program with the airlines. Who is on first? Who has got the responsibility? Is that a wrong conclusion on my part? How would you respond to that?

Mr. Dempsey first.

Mr. DEMPSEY. Well, Mr. Chairman, I would say that your facts are right but your conclusion I would probably disagree with, in that, yes, it results or appears to result in some ridiculous results, but I do not think the answer is to try to bring the administration of CAPPS behavioral rules into the government. The government sets the rules, it changes them from time to time based upon new information, it tries to refine them, it provides them to the airlines.

As I understand it, application of CAPPS behavioral rules requires a lot of information—passenger name record information,

frequent flier information, some historical data—data that the government really cannot collect easily, cannot digest, cannot hold, would have a hard time. I think you might by bringing that in government produce a worse result, produce a gridlock.

So I would say refine it, and it clearly needs to be refined, work with the airlines on those implementation questions, absolutely, but basically keep the current structure.

Mr. LUNGREN. Mr. Rosenzweig?

Mr. ROSENZWEIG. Well, as you will gather, I am somewhat more skeptical that the CAPPS I rules have a continued vitality. To the extent that they do, though, I would agree, I think, with Mr. Dempsey that they are better placed with the airlines. They are behavioral rules, and it is classified and so on, reading in the public record, but they are buying with cash, flying one way, and that is the type of personal behavior that is precisely the type of privacy-related material that we want to try if we can to keep out of governmental databases.

So to the extent that we are talking not about factual record data, like a date of birth or a name that is a matter of public record that is okay, in my judgment, to take into a government database but rules about how often you fly, where you go frequently, whether you are paying cash or credit, that sort of thing. That would seem to me to raise more significant privacy concerns, and it would be better to be kept in the commercial data space rather than in the governmental data space.

Mr. LUNGREN. Mr. May?

Mr. MAY. Actually, Mr. Chairman, we think that CAPPS I, because it looks at behavioral activity, does present some opportunities down the road for continued good security. We do not think that the CAPPS Program, as it is currently crafted, all of the elements are necessarily as well done as they should be. At the end of the day, it has to be a government designed program we think we can continue to implement.

But, remember, when we tag somebody for behavioral activity, it really then is up to the?what we are doing is we are making them a selectee, and they are going to be subject to additional scrutiny. I think what we are talking about today, Secure Flight, is an equally important part of the process, and I think that should, as Congress has said and others have said, be a function of TSA.

I think to the extent it is improved upon and combined with some behavioral checks, I think it will be overall a much better system.

Mr. LUNGREN. Let me just ask the three of you, and I do not mean to leave you out, Mr. Anderson, but the question of not having the proper information to do these checks, that is, you have got two different groups of characteristics, how much would it improve the systems that we are talking about here if you had in addition to the name the date of birth, and maybe even birthplace.

Mr. DEMPSEY. It seems to be that the evidence is that adding date of birth for the watch list matching most watch list entries have at least name and date of birth, and so to make a match that is what you need, unless you can augment the watch list with additional data.

Mr. ROSENZWEIG. There is every reason to think that something simple like that will work. The best analogy that I can think of that I have seen in the literature is by Dr. Latanya Sweeney of Carnegie Mellon who has demonstrated pretty effectively that zip code and date of birth uniquely identify about 97 percent of the people in the world—or in American, I should say, because she applied it in an American database. The only exceptions to that turn out to be collect campuses where there is a very high concentration of people with a very narrow birth range, all with the same zip code.

So that suggests that name and date of birth, name, date of birth and zip code would be pretty darn close to effective in uniquely identifying each individual.

Mr. LUNGREN. My time is up, but, Mr. May, on that, would that cause any considerable difficulty to the airlines to gather that information?

Mr. MAY. I think that is doable, but what I would like to point out, Mr. Chairman, two things. One, TSA is not the only one that asks to collect information from the airlines. There are other parts of DHS that do that. Whatever system we have let's make sure it is standardized across the whole board.

Mr. LUNGREN. I thank the gentlemen for their comments.

The Chair now recognizes the Ranking Member of the full committee, Mr. Thompson, for 5 minutes.

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

Following up on the questions, it is kind of related to Mr. Anderson's situation, but if I give those three forms of identification, under normal procedure, that would suffice for getting me off the list, am I correct?

Mr. ROSENZWEIG. Provided that the list itself allows the clearance, the fact that you are cleared to propagate to all the users, which is one of the reasons to take it in-house at TSA, if we have hypothetically Mr. Anderson's name, date of birth and zip code, that uniquely identifies him, and if he is carrying something that has those three pieces of information on it, that should be a simple Google search-like click-through methodology. I mean, it is not technologically—

Mr. DICKS. On what document do you have your zip code?

Mr. ROSENZWEIG. Well, name and date of birth you have on your driver's license, and it is true that we do not normally carry zip codes. I offered that as a hypothetical additional one.

Mr. THOMPSON. Well, I guess going forward to the next step, if I am picked up under Secure Flight, what redress will I have to get off the list?

Mr. Dempsey?

Mr. DEMPSEY. Well, that is one of the unanswered questions, okay? The TSA has not yet fully spelled out what its redress process will look like. It has said it knows it needs one, it needs to be robust, it needs to be effective, it needs to be user friendly. Getting from here to there requires some more work.

I think there is apparently a John Anderson or somebody with a name like John Anderson on the watch list. You are never going to take John Anderson off the watch list. Presumably, he is on

there correctly, although we do need to reverify and revet, I believe, on a yearly basis the names on the watch list.

But the question is showing John Anderson but not this John Anderson, and that is where the additional forms of identification come in and some way to build into the system, and I do not think it is quite as easy as people have talked about so far, the ability to say, "Stop all John Andersons except this John Anderson," and then every other John Anderson goes through the process.

Mr. THOMPSON. What about the middle initial? I mean, that has got a get a few of them out of the list.

Mr. DEMPSEY. Then you have to start collecting middle name on passengers, and you have to start having middle name or middle initial in the watch list.

Mr. MAY. The point that was just made is critically important, Congressman. It is as important to have fully identified individuals on the watch list as it is to be able to check with the individual passengers.

Mr. DICKS. So in other words, if you just have John Anderson on the watch list, then every John Anderson is in trouble, because they cannot distinguish between that and—

Mr. MAY. Right. We need to—

Mr. DEMPSEY. Well, and it is worse than that, Congressman, because it is possible they have J. Anderson, and when they search they are not going to only search for Anderson, S–O–N, but they are going to search for Andersen, S–E–N, and they may search for John and James and Jack and Johnny, and they may search for an Anderson with two As or Ss, et cetera. That is the way the searching of names works. That is why name search alone is so unreliable.

Mr. ROSENZWEIG. Just to add a couple points, Mr. Dicks, I just checked, my driver's license actually has my zip code on it too.

Mr. DICKS. It also has your social security number on it.

Mr. ROSENZWEIG. Actually, in D.C., it does, yes. So it uniquely identifies me in several ways. But the point you asked, Mr. Thompson, is actually the hardest question, which is what process are we going to allow somebody to get off the list, the redress process. It is pretty easy for people like Mr. Anderson who are wrongly listed, who are not the John Anderson they mean.

The tough question, the really hard question is, what if he is the guy that they meant but he contends he should not be on the list? There is a John Anderson that we have some suspicion about, presumably. What if that guy shows up and say, "No, I am an innocent bricklayer from Terre Haute?

How do we test it to allow—there has to be some adversarial process, clearly, but it cannot be a fully transparent process, because often the reason that John Anderson is on the list is because of some national security concern that cannot be fully disclosed. It is a very intractable problem.

Mr. THOMPSON. I guess the other point is, do you think we are ready for the demonstration given what we are hearing here today?

Mr. DEMPSEY. I do not think so.

Mr. MAY. Congressmen, I do not know that we are ready for the demonstration, but I think it is only when you get to a demonstration and it is what it is, it is a demonstration, it is a test, that you

begin to identify some of the problems that you are going to face in putting it out live, if you will. And so I think you need to go through that phase of it.

I do not think TSA is ready right this minute, but I would hope they can become ready soon, recognizing that there are going to be some problems that show up that will have to be resolved. But it is only when you test it that you find that out for certain.

Mr. LUNGREN. Gentleman's time has expired.

The Chair would now recognize the chairman of the full committee, Mr. Cox, for 5 minutes.

Mr. COX. Thank you, Mr. Chairman.

Thank you once again to all of our witnesses. This is a very important hearing, and I want to particularly thank a former colleague, Mr. Anderson, for coming and sharing your personal experience.

I take it you have not flown since the Delta experience.

Mr. ANDERSON. No, I have not.

Mr. COX. So you do not know what would happen if you tried to do this again.

Mr. ANDERSON. I do not.

Mr. DICKS. They just told him.

[Laughter.]

Mr. COX. Mr. Rosenzweig, you pointed out in your testimony that each airline administers the watch list matching differently and that there is a high variability in the matching operational methodology and that there is no single common standard for defining watch list match, neither is there sharing among the carriers on a routine basis of all of this information. So isn't it likely that Delta did not take that information and spread it all around the industry?

Mr. ROSENZWEIG. Well, I think it is quite likely.

Mr. COX. So that if John Anderson wants to fly to Germany again but takes a different airline, he is going to have to call up his congressman and start from scratch and go through this whole routine all over again, isn't he?

Mr. ROSENZWEIG. Well, I would hope not, and it might have?

Mr. COX. Well, I would hope not too, but what reason do we have to think that this would not happen again?

Mr. DEMPSEY. Congressman, Mr. Chairman, I think that is part of the reason for bringing the watch listing process into the government, to do the matching on a centralized basis in the government, both in order to use the best name-matching technology, whatever that might be, and it has not been determined yet—

Mr. COX. Well, I want to go even further—

Mr. DEMPSEY. —and then, secondly—

Mr. COX. —and ask why it is that we think that if there are people who have been blessed by their parents with names like John Anderson in the world that we are going to single them out with that kind of a system?

I mean, we have two objectives here. One is, and it is the primary objective, to find out which, if any, of the people that are boarding airplanes are terrorists. The other, which is ancillary to that primary purpose, is to reduce the size of the haystack that we

are sifting through so that we can focus our energies and our attention on the right people.

Now, Chairman Lungren pointed out he is concerned about infants being sent for secondary screening. There is no reason on Earth if we use CAPPS I that we are not going to look at infants because infants may well have had their tickets purchased with cash or may well have made a last-minute change in their reservation and bought a one-way ticket. Those kinds of things, dumb criteria, if you will, like that are going to focus us on the wrong people. Whereas, what we ought to be doing is reducing the size of that haystack.

We have good information about people like John Anderson. Unfortunately, we do not always have good information about the terrorists. But what we can do is use the good information we have about Mr. Anderson to let him go through the airport quickly, reduce the size of the haystack and focus the attention on actual terrorists or suspected terrorists.

Mr. DEMPSEY. Mr. Chairman—

Mr. COX. We will never be able to do that if we are relying on such primitive information as John Anderson. We have got a lot more information about Mr. Anderson, which he discovered himself when he Googled himself.

Mr. DEMPSEY. Mr. Chairman, in terms of the infants and the grandmothers, I think a huge issue there is training and discretion and the judgment of the screeners. After all—

Mr. COX. Well, let me ask Mr. May, because it was suggested a moment ago by Mr. Dempsey that this is an airline issue that—or maybe it was Chairman Lungren that said this—that the airlines are the ones that are supposed to be not screening the infant. Why does this persist?

Mr. MAY. I think it persists because we are using behavioral criteria that are established by TSA. We are not in the position of making the judgment as to who should or should not. We are in the position of enforcing the boarding pass identification based on those behavioral characteristics.

They then go to the screening process, and if they are identified as a selectee based on those CAPPS I criteria, then it is up to TSA. I think it absolutely should be that if somebody has been identified as a selectee because of a behavioral characteristic, that TSA can look and see that it is an 11-month-old infant and that relieves the responsibility right there, as it would a 95-year-old grandmother.

Mr. COX. Let me ask my final question, because I have less than a minute left.

Mr. Anderson, you have heard about Registered Traveler, a voluntary program that you might sign up for in order to avoid all of this hassle. What kind of incentive would you need as a traveler in order to want to sign up for such a program?

Mr. ANDERSON. Well, I do not think I would ask for frequent flyer miles or any compensation of that kind. I think if it were available, if such a program were available, I would rather willingly cooperate.

I do not deny there is a huge problem out there of eliminating the possibility that we are going to have another terrorist hijacking, and I would not want to stand in the way of all efforts that

are made to try to screen out people, but a voluntary sign-up of some kind to eliminate, just as we voluntarily engaged in this program to get on the no-call list, not to be bothered during dinner hour by people—

Mr. COX. A national no wait in line list.

Mr. ANDERSON. Exactly, some national list of that kind where you could relatively easily say, "Yes, I subscribe to this," and then get the clearance you need.

Mr. COX. Thank you very much. This has been an excellent panel, and I am going to continue to listen intently.

Thank you, Mr. Chairman.

Mr. LUNGREN. I thank you.

The gentleman from Washington, Mr. Dicks, is recognized for 5 minutes, in which time that he wants to give to the chairman he can.

Mr. DICKS. That is Mr. Thompson.

Tell me what Secure Flight is going to be about. Explain what Secure Flight is going to be.

Mr. DEMPSEY. Secure Flight is the matching of passenger names with a list of known or suspected terrorists in order to determine who deserves secondary screening in addition to the metal detector and luggage x-ray.

Mr. DICKS. And what list is this passenger list from the government—this is a government list, I take it.

Mr. DEMPSEY. Yes, sir.

Mr. DICKS. What list is this?

Mr. DEMPSEY. On the next panel is Justin Oberman, who is head of the Office of Credentialing and Vetting at TSA, and he can answer those, but I will say that the list is the consolidated—it is a subset of the consolidated watch list managed by the FBI from 11 or 12 watch lists that the government had been using prior to 9/11. The Terrorist Screening Center was created at the FBI to bring together these disparate watch lists.

Mr. DICKS. They still have not got this done, you know.

Mr. DEMPSEY. Well, to some extent—honestly, Congressman, I believe they have made progress on this. It is an incomplete system, it is better than it was on 9/11, although we read in the paper this morning that the State Department has not been using it to screen applicants for passports, which is bizarre. But, look, we have put a lot of effort into trying to figure out who are the terrorists.

Mr. DICKS. But I am told that even on this list there are certain names that are left off.

Mr. DEMPSEY. There are both names that are on the list that should not be, and there are names that should be on the list that are not, that is correct.

Mr. DICKS. Explain that. Can you explain that?

Mr. ROSENZWEIG. I guess the answer is, nothing is perfect. I mean, we have as a goal the creation of a unified watch list, but to expect, especially in the context of intelligence information, which is often indefinite and hazy, that it is a perfect list is unrealistic. If your objective is only to implement perfect systems, we will never implement any.

Mr. DEMPSEY. But some of the flaws here, Congressman, one day the employee at the FBI who was responsible for loading the names into the list and that person's backup were both out. Therefore, that day no new names were loaded into the list and when people came to work the next day they did not go back and fill. So that is one reason that the Inspector General found as to why not all the lists that should be on the list are not there.

Mr. DICKS. So, Jim, what is your major concern here? From ATA's perspective, you were kind of gentle, I noticed, in your testimony. You said it was not perfect but you hoped it would get better. What are you mainly concerned about here?

Mr. MAY. Congressman Dicks, I think we want to see, number one, the federal Government take over the business of matching names on whichever list or combination of lists are going to be used. Number two, I think we want to have a simplified data collection process that, whether it is CBP or TSA or anybody else that is collecting information for the airlines, it is consistent fields of information.

Number three, I think we need to have discussions with TSA, CBP and others, it has been discussed here that we have a number of different ways to implement the program based on different computer systems, carriers, things of that sort. Let us have those conversations so that we know how that information is going to be managed.

Number four, do not forget that we are not the sole collectors of information. Travel agents, for example, collect information, and we may not even be in receipt of a lot of the required information on a number of passengers until they check in with us immediately prior to their flight on a connecting flight from another airline.

Mr. DICKS. So that is where you say on the flight coming into the United States. It does sound ludicrous that we check these things 15 minutes after the flight leaves. I mean, if you have got the terrorist on there and he is, whatever, that is disconcerting. And then we have to land up in Maine or somewhere and get the person off.

Mr. MAY. That is correct, and that is why we suggest a real-time process where you get a board/no board as we get that information in.

Mr. DICKS. But it should be before the plane leaves, shouldn't it, I mean, in a perfect world?

Mr. MAY. In a perfect world, it should be before the plane leaves, but we do not live or operate in a perfect world.

Mr. DICKS. Would a real-time system allow you to do it before the plane leaves?

Mr. MAY. A real-time system would allow us to do it better than we do it today. Do not forget that if we had it on an hour in advance, it still takes them 4 hours to process that information. When they have a conflict between John B. Anderson, III and John Anderson, it still is a human being that sits down and starts to look at other information to try and correct that. And in the final analysis, the airlines would far prefer to have some planes turned around over the Atlantic than have the huge delays that would be required of processing information on all of those passengers, all of the time prior to departure.

Mr. DICKS. So in a real-time system, it still would take 4 hours.

Mr. MAY. Right now it is taking—we think it is taking—

Mr. DICKS. That is why on these 8-or 9-hour flights they get it—

Mr. MAY. Right. Right. So get a real-time system that allows us to put that information in 2 hours in advance, for example. When we have it an hour in advance, a half hour in advance, there is still probably going to be some passengers that are not prescreened prior to getting on. Now, they are going to be prescreened according to CAPPS I. They can be run against a watch list, et cetera. But in depth APIS screening will not necessarily take place for every single passenger, but that is a risk we will take because we think the disruption to the system of a mandatory 60 minutes prior to departure is going to be far greater.

Mr. DICKS. Thank you, Mr. Chairman.

Mr. LUNGREN. The Chair now recognizes Mr. Linder for 5 minutes.

Mr. LINDER. Thank you, Mr. Chairman.

Mr. Dempsey, you said that it is clear that the terrorists are still seeking access to airliners. Where do you get that information?

Mr. DEMPSEY. Well, I am not privy to any intelligence but it seems to me that it is one of the most powerful targets that they have. They have shown—

Mr. LINDER. Have more people died on airlines or trains?

Mr. DEMPSEY. Excuse me, sir?

Mr. LINDER. Have more people died on airlines or trains?

Mr. DEMPSEY. I honestly do not know the answer to that, but we have had some spectacular losses of life on airplanes.

Mr. LINDER. Do you think another airplane will ever be allowed to go into a building?

Mr. DEMPSEY. Not if the passengers can help it.

Mr. LINDER. Do you think the passengers will help it?

Mr. DEMPSEY. Yes, sir. They may die in the process, but they are going to probably rise up and prevent it.

Mr. LINDER. That is correct. And the value of the airliner on September 11 was that it was full of fuel and it was come to allow to fly into a building because the passengers up to that point had believed they were just going to be taken off somewhere. And it was spectacular because the jet fuel burned down the buildings.

If it is the case that I think it is that the terrorists are looking for spectacular financial events, it does not seem much in their interest to just take down one airliner. And they can do that today by just putting a bomb in the cargo hold.

Mr. DEMPSEY. When I fly on airplanes, I hope people have not given up on protecting airplanes.

Mr. LINDER. We had 690 million passenger flights on airlines in 2004, and we spent $5 billion on that. We have 9 billion passenger rides on trains, we spend one-half of 1 percent of the budget on that. Do you think that is fair?

Mr. DEMPSEY. Well, I do think that you raise the question of risk assessment and prioritization, which is absolutely part of this. We obviously had a terrorist train bombing or subway bombing, commuter train bombing in Madrid. So our security system must look at and evaluate all of those risks. Whether too much money has been spent on air transport to that exclusion of other forms of transport is something that I am not going to offer an opinion on.

I do stand by my position that terrorists see airplanes as potent targets, and if they can, they will take one and they will either blow it up or crash it. And we need to keep terrorists off of airplanes, which means we need to screen passengers, and we need to do so in a cost-effective way, I agree with you entirely.

Mr. LINDER. I do not think it really matters just who is on an airplane, because fake IDs are so easy to get in this day and age that anybody—no terrorists are going to get on there and identify themselves correctly and tell you where he is from.

Mr. DEMPSEY. Most of the 9/11 hijackers flew under their true names.

Mr. LINDER. That was pre–9/11. That was pre–9/11.

Mr. DEMPSEY. It is an excellent point, Congressman. The GAO noted in its report that identity theft does pose a serious challenge to screening. We have efforts underway, separate efforts, to improve the quality of identification documents. Identity theft and fake IDs pose a risk in a number of contexts. If we were to vet train passengers, the same problem would be posed there.

So the fact that we do not have a perfect ID system, to me, does not say that we should not try to figure out who is getting on an airplane.

Mr. LINDER. If we take this system and move it to the train system, we would make a huge mistake, because this one does not work, for starters.

Mr. May, let me ask you something.

Mr. DEMPSEY. Congressman, just let me say I agree that this is not working yet and it should not be extended to any other forms of transportation until we can prove that it works in the air transport context.

Mr. LINDER. It appears to be a wholly owned subsidiary, the airline industry.

Mr. May, nobody has mentioned biometrics here. In your judgment, if we had a background screening and I had a fingernail print, shouldn't I be able to just walk on that plane?

Mr. MAY. Mr. Linder, we have long supported the concept of Registered Traveler because we think if you have a robust Registered Traveler database using biometrics and they use iris and fingerprint, that it removes the number of people or a number of people that would otherwise be potential selectees.

Mr. LINDER. But the ones we have right now they go through and identify themselves with a fingerprint at Reagan National, still go through the magnetometer, still take off their shoes—

Mr. MAY. That was exactly the point of my testimony. We have to have TSA identify the benefits for belonging to that program, for providing the biometric information so that you do not have to take your computer out, you do not have to take your shoes off, you do not have to take your outer garment off, et cetera, so you can quickly move through the process. And then you have to have those six test programs learn how to talk to one another as just one other additional step in the process.

Mr. LINDER. Thank you, Mr. Chairman.

Mr. LUNGREN. The Chair now recognizes the gentlelady from California, Ms. Sanchez, for 5 minutes.

Ms. SANCHEZ. Thank you, Mr. Chairman, and I am sorry for having arrived late. I was caught in another committee meeting. And I did not get to hear the testimony of all of our gentlemen before us, but I do have one question.

I have a constituent, Bob Lewis, has a regular sounding name, a businessman, he goes to the airport quite a bit. And every single time he gets stopped because there is a Bob Lewis on the list. Now, he is not that Bob Lewis.

So with respect to that, he has talked to all of the agencies, he has finally gotten a letter that says he is not that Bob Lewis, so now he shows up to LAX and it can be normal procedure of showing them the letter and that is fine and goes through and takes off his shoes like everybody else or sometimes he is set aside for 4 hours, missing his flight because somebody is not trained or somebody does not believe the letter or something is going on. I mean, this is an occurrence that happens over and over to this gentleman.

So my question is, what is the process to stop that from happening currently, because it is very aggravating. And he is not the only I have but this is not a—I mean, believe me, I have plenty of Middle Easterners and Muslims. I have the largest mosque in California in my district. But I am talking about just a regular Anglo–Saxon community leader type of person.

Mr. ROSENZWEIG. Actually, ma'am, I think that that is probably the best argument for Secure Flight that you could make. The reason he keeps getting stopped is because the current distributed network system is not just distributed but disconnected. So they cannot disambiguate him from the other Bob Lewis, was it?

Ms. SANCHEZ. Bob Lewis.

Mr. ROSENZWEIG. They cannot disambiguate him from the other Bob Lewis. He is not that Bob Lewis. That Bob Lewis may be 42 and Hispanic from El Toro and he is Anglo–Saxon and 37 from El Centro.

Ms. SANCHEZ. He wishes he was 37.

Mr. ROSENZWEIG. Okay. But the point is that in the disconnected system we have now, I mean, it is absurd.

Ms. SANCHEZ. But he has been corrected. He has been corrected with the letter, so we are going back to this training issue.

Mr. ROSENZWEIG. Well, it is a training issue, but it is absurd that we have a system where the correction has to be a hard copy that he has to carry with him, right?

Ms. SANCHEZ. But even when he carries it with him the problem is still whoever has not been trained correctly.

Mr. ROSENZWEIG. That is true. That is true. And obviously training and implementation issues need to be addressed as we transition. I guess the point of what I would take away from your experience is that if we actually transition to a better system, the training problems diminish substantially. I mean, let's be honest, there are 43,000 TSA people. You are never going to have all of them trained perfectly. There is a lot of turnover. We cannot expect human systems to be error free, much as we would like it to. We can expect better of automated systems that use additional data about the good Bob Lewis to distinguish him.

Ms. SANCHEZ. So the Secure Flight would have the real information on the good Bob Lewis in there, "Do not stop this guy, he looks like this."

Mr. ROSENZWEIG. If properly implemented, I believe that the—and you should ask Mr. Oberman back there when he comes—

Ms. SANCHEZ. Well, I will when he comes up.

Mr. ROSENZWEIG. —but if properly implemented the good Secure Flight system should have identification about the good Bob Lewis, maybe his biometrics, probably more likely simply his date of birth, which I am sure is different from whoever the bad Bob Lewis is, that he carries with him already on his driver's license. And if that is all that it takes to distinguish the two, then the good Bob Lewis will be carrying with him not a letter but a driver's license that just type it in, bam, he is the good John B. Anderson, not the bad John B. Anderson.

It can work. It does not yet, to be sure.

Ms. SANCHEZ. Any of the rest of you have a comment?

Mr. MAY. I would simply note, as we said with Mr. Linder a minute ago, if you have got biometrics attached to a Registered Traveler Program that has absolute positive benefits for the traveler, Bob Lewis could become a registered traveler with biometrics and breeze through the system on a regular basis. And I think that needs to be a component of the overall process.

Ms. SANCHEZ. Well, just to mention that so far it is only one airline at LAX at a certain terminal, in a certain way, and so, you know.

Mr. MAY. We agree with you. And that program does not talk to the one in Minneapolis, it does not talk to the one at Washington National and so forth.

Ms. SANCHEZ. Exactly. A lot of work to be done.

Thank you, Mr. Chairman.

Mr. LUNGREN. The Chair recognizes the gentlelady from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman. And I appreciate this hearing because I think we need to examine what we are doing here from really the very beginning. We are spending a lot of money, not only in terms of expenditures, but the public is spending a lot of money in terms of their time, and the question is, what are we getting for that investment? I guess my current operating belief is not too much.

How many names are on the watch list, do you know, Mr. May? Anyone?

Mr. DEMPSEY. About 200,000.

Ms. LOFGREN. Now, do we believe that there are 200,000 people who want to either blow up a plane or hijack a plane?

Mr. DEMPSEY. No.

Ms. LOFGREN. So we have got a lot of data there that we are checking the bad John Andersons or the bad Bob Lewis's, but there is no reason at all to believe they are going to hijack a plane or blow it up.

Mr. DEMPSEY. Congresswoman, let me just also clarify that a little bit further. The consolidated terrorist screening database has, according to the DOJ Inspector General's report, I think currently about 260,000 names.

Ms. LOFGREN. Well, reclaiming—

Mr. DEMPSEY. But then only a subset of that is used as the no-fly and selectee lists.

Ms. LOFGREN. And that is about 37,000?

Mr. DEMPSEY. Right.

Ms. LOFGREN. And we do not believe there are 30,000 people on that list that intend to blow themselves up.

Mr. DEMPSEY. No, but what we are talking here about, I believe, Congresswoman, and your point is 100 percent, as Mr. Linder's point, is 100 percent correct, we do need to do a little baseline questioning here. But these are people who are being referred for secondary screening.

Ms. LOFGREN. Well, it is worse than that. I will just give you a little personal story. My husband and I were in Los Angeles and we were going to fly back to San Jose on Southwest Airlines. It was a nightmare. I mean, it was like a two and half hour security line. I went fine. We found a line to the kiosk, got my little boarding pass, and then we could not get John's boarding pass. And finally we found?we are in another hour-long line and it is a J. Collins is on the list.

I will tell you to get cleared by the Southwest people took like—they said, "Oh, well, you are not him," and gave a boarding pass. But there is no way to get off the list, and it is not him, and I do not know who the J. Collins is, whether this is somebody who really would blow themselves up, but Senator Kennedy went through it, Mr. Lewis went through it, Mr. Anderson went through it, my husband is going through it, and it bears no relationship to keeping the nation safe. So that is a stupid system, and we are spending a lot of money on it, and it does not make us any safer at all.

So I think we need to start from the very beginning. What is this list and how does it inform us about who is really going to be a threat to the nation? And if we have a small group of people who we have reason to believe are going to blow themselves up or hijack and airplane, it is not going to be 37,000 people, it is going to be a much smaller group, and then we should look at those people pretty carefully when they try and board an airplane. But the system we have now, and I cannot believe and I heard it took 4 hours to do a database search. I mean, who is doing our software here? I mean, that is astonishing.

So I just think this system is—you know, we always look at the last problem not the next problem. We are throwing resources at this system foolishly. We are not providing value, we are not providing safety, and we are completely ignoring the exposure we have in other transportation modes that is likely to be the next target.

So we can do biometrics. I mean, the chairman and I had all of our fingerprints taken when we sworn into the state bar. The government has my fingerprints. But until we know what we are sorting for, I think we are just causing a lot of problems here.

Mr. ROSENZWEIG. Can I just gently disagree with you slightly?

Ms. LOFGREN. Certainly.

Mr. ROSENZWEIG. And, certainly, the person you should talk to is Donna Bucella who runs the Terrorist Screening Center who we heard from in the Privacy Committee that I am on a couple weeks ago, and she can do much better at this. But it strikes me that

37,000 is not as big a number as you think it is, because it is not 37,000 Americans. It is 37,000 people out of 3 billion worldwide, which is—I was trying to do the math while you were talking, but I think it is one one-hundredth of 1 percent.

And if you ask the question, do we think that there are 37,000 people worldwide who are bent on terrorist impulses, I have no personal knowledge. I do not get any classified briefings, but I am going to guess that there probably is that many that we know about.

Ms. LOFGREN. I see that my time has expired, but, Mr. Chairman, I think at a future hearing and maybe even in a classified session it would be of value to explore what this list is and what it is made up of and what kind of information is provided, just as a baseline for the beginning of the discussion.

I yield back and thank the chairman for his recognition.

Mr. LUNGREN. I thank the gentlelady, and that is something I think we ought to do. And I would just say that that list changes from day to day. And without revealing any classified information, in investigations we know from Judiciary Committee experience in the intelligence area sometimes someone is put on a list of suspicion based on the fact that they had lunch with someone that we know is a known suspected terrorist. And until further investigation reveals them not to be someone, they would probably be on that list. So it is an expanding and contracting target.

And I think our real question is, how do we get people such as your husband and Mr. Anderson who are clearly not the person that is meant to be on that list, how do we clear them, and do we utilize, for instance, commercial information? Do we use commercial databases? And if that is the case, does the government have that or do we query those as opposed to having the government set up their own systems, which brings up questions of privacy? And until we create that context for discussion, you will have criticism of the government ever looking at commercial databases.

And I think that is part of our inquiry here. We have tried in this hearing to set up the dimensions of the problem, and how do you get out of that problem I think is the next inquiry, and that goes into the question of databases and who utilizes the databases, for what purpose, and who keeps them? And in which way do we protect privacy to a greater extent? So I appreciate—

Ms. LOFGREN. Would the gentleman yield for—

Mr. LUNGREN. Yes.

Ms. LOFGREN. —for a comment, because I think what is missing here is the connection of information to risk. There are people on that list, I will use an Ireland example, people who donate to the widows and orphans but it might actually be the IRA and they could end up on that list and it has nothing to do with whether they are going to blow themselves up on an airplane. And so the information does not match to the risk, and we are spending a huge amount of money, consequently.

Mr. LUNGREN. That is part of our inquiry, but the other part is, as I suggest, if you do have a defined number of people on a list, and yet we know John B. Anderson is not that person, how do we create a system that is more efficient in removing this John B. Anderson, his progeny and so forth, from that? And I think those two

areas of inquiry, and then on top of that how do we protect appropriate privacy concerns?

Mr. DEMPSEY. Mr. Chairman, if I could just comment upon that for one second because everything that Congresswoman Lofgren has said I agree with. Last December, Congress required the administration to report by the end of this month on what are the criteria, how do you get on, how do you get off? As far as I know, that report has not yet been submitted. I certainly have not seen any reports about it. But we have been over this ground once before, but we have to o over it again.

The Intel Reform Act also said that that watch list should have better information about how you got there and why you are there and what level of risk you pose, because I agree with you entirely. Whether it is 260,000 or 37,000, there are different levels of suspicion there, and, clearly, when that consolidated watch list was first created, and the TSC admits this, it was overbroad. They dumped a lot of stuff in there because they were in a hurry and they did not want to miss something.

But now we are seeing the consequences of that, and it is time to go back and reconsider who is in there, why, what is the validity of the information, and then what is the quality of that identifying information so we can begin to tell one person from another.

Mr. LUNGREN. The gentlelady from Texas wish to inquire? Okay. The gentlelady is recognized for 5 minutes.

Ms. JACKSON-LEE. I thank the chairman for this hearing, and I guess I just want to pursue the line of questioning that my colleagues have been, and I will ask a broad question to all of you.

We are a team dealing with homeland security, and the more precise we can be, the more effective that we will be, in addition to the watch list and the backlog that I understand in terms of refining the watch list. Many of us have had constituents raise questions about that. Are you in need of more resources, more technology, more training? And out of the watch list, can you account for me any arrests or any terrorist that was deterred or any act that was deterred because we have the existence of a watch list?

Why don't I let whoever—

Mr. DEMPSEY. I am sorry, Congresswoman, none of us represent the watch list, none of us work for the government, so I do not know that any of us are in a position to answer that question. The next panel does have a witness from the government.

Ms. JACKSON-LEE. Do you have any comment about the existence of a watch list?

Mr. DEMPSEY. Well, I will say that part of the effort to prevent and combat terrorism is to identify terrorists, and we have an effort to identify them. There are various screening points in life, in society where individuals are seeking a government benefit or in this case to travel, and there is an interesting question there, where we have to determine is the person entitled to enter this country? And terrorists are not entitled to enter this country. Is the person entitled to a visa? Terrorists are prohibited from acquiring visas. So we try to figure out who the terrorists are and are they entitled to certain benefits or rights.

Ms. JACKSON-LEE. But we need to be right in doing so, and I appreciate you trying to take a stab at a question that you think you might not be prepared for.

Let me just go right to Mr. Anderson, and I am sure you have been probed extensively, Congressman. I am delighted to see you.

Mr. ANDERSON. Thank you.

Ms. JACKSON-LEE. And we all owe you a debt of gratitude for your service. But you have lived in different periods of our country's history, and we all know how we had to change our thought processes after 9/11, but as the constitutionalist that you are, a person who obviously applauded and utilized the freedom that this country represents, tell us the stress, the strain and the enormous difficulty that you had in clearing your name.

And when we talk about insurance issues, we talk about risks. Insurers will say, "I am willing to give this certain amount or even products based upon we are willing to accept this amount of loss on this product." Is it equal to what safety we are getting by what you had to go through or the existence of lists like this?

Mr. ANDERSON. Well, I think the general consensus, and I would not presume to speak for the other members of the panel this morning who have far more expertise than I, really, on a day-to-day basis of dealing with this problem, but I think there has been a consensus that there is definitely overbreadth in the list and that there are serious questions as to whether or not the methods that are employed to compile that list comport with recognition, as it should have for standards of privacy and indeed whether or not the standards that are employed to compile the list are even very sensible and reasonable and that the system is broken and that it needs to be reworked.

No one challenges, as I think is also implicit in your question, the need to protect ourselves against terrorists boarding airplanes and all the rest, but we cannot tolerate a system that involves your fellow congresswoman testified to the difficulty that she and her husband have had.

Ms. JACKSON-LEE. Well, it cries out for action.

Mr. ANDERSON. I am only one, I think, of literally many, many people who feel that this system is very badly flawed, and this committee has the responsibility, and I am happy that they see it the same way, of undertaking to find out what can be done to correct the present system.

Ms. JACKSON-LEE. Thank you very much.

Mr. LUNGREN. Thank you.

Ms. JACKSON-LEE. Thank you very much.

Mr. LUNGREN. I again thank all the witnesses for their testimony. It has been a very interesting hearing. You are helping us in our inquiry as to where we are and where we wish to go. The witnesses are excused, and I would call up our second panel for testimony.

The Chair now recognizes Mr. Justin Oberman, the Assistant Administrator for Secure Flight and Registered Traveler Program at the Department of Homeland Security to testify.

And I would say, Mr. Oberman, that your written testimony will be put in the record in its entirety, and we would ask you to make

your oral presentation in 5 minutes, and then we will have some questions for you.

Thank you for being here.

STATEMENT OF JUSTIN OBERMAN, ASSISTANT ADMINISTRATOR, SECURE FLIGHT AND REGISTERED TRAVELER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. OBERMAN. Thank you, Chairman Lungren, for calling this hearing. Chairman Cox, Congresswoman Sanchez, Congressman Thompson, pleasure to be here to discuss one of the most important programs we are trying to launch at the Department of Homeland Security.

As you know, the issue of protecting security on domestic aviation is one of the nearest and dearest threats to 9/11 and one of our most important missions, not only at TSA but also at the Department.

As you also know, the 9/11 Commission recommended that the government assume the responsibility for checking domestic passengers against terrorist watch lists, and of course the Congress built on that recommendation in the Intel Reform Act last December and also required us to stand up this system, and of course that is exactly what we are doing.

We have been in a testing and planning phase since we launched the program last September and have done quite a bit of work to define our capabilities as well as areas where additional progress is needed. Our testing, for example, has shown that our existing technology does have the ability to vet the names of 1.8 million people who fly in the United States every day and to do so far more accurately than the air carriers do today, particularly if we have every passenger's full name and date of birth.

As you also know, we are conducting a test to determine whether the use of commercially available information can assist us in carrying out our pre-screening function, particularly with respect to making our watch list matching capability even more accurate and also to see if we can get at the critical issue mentioned by several members today regarding verifying the identities of people who fly.

In addition to that, the test also looked at our ability to assume the responsibility for CAPPS I from the airlines, and it was a very useful test because it showed that it was in fact very difficult for us to take that over for the reasons that I think Mr. Dempsey alluded to, that information far beyond what is in the passenger record is required to run CAPPS I.

Partly in response to that, the Department amended the CAPPS I rules in January and gave the carriers 90 days to make those changes. That 90 days, of course, has come and gone, and we have seen selectee rates due to CAPPS I drop significantly across the industry. The major carriers have a CAPPS I selectee rate of under 10 percent, and the regional and low-cost airlines who are disproportionately impacted by criteria that are publicly known, such as paying for tickets in cash and flying one way, have seen their selectee rates drop in some cases by half or more as a result of the changes that TSA authorized in January. That is a big improvement.

I do want to address, though, several other key issues right now and hopefully during the course of my testimony that I think are very important and of course are on the minds of members of the committee and others, and they include the following: Number one is our budgetary situation. We are in a very difficult situation with respect to funding for Secure Flight. The President requested $60 million for fiscal year 2005 and we were funded at $35 million. That is a 40 percent reduction, which required us to significantly curtail our plans for the current fiscal year.

Furthermore, the President's request for 2006 is $81 million, and the House mark, which is obviously now public, is at $66 million. That is about a 20 percent cut. The Senate mark is at $56 million, which is about a 30 percent cut.

And what I can tell you is that if the enacted level is less than what the President requested, our ability to meet our timelines, which we have set ourselves and as well are required by the Intel Reform Act, will be in serious jeopardy. The program needs to be funded at the President's requested level for us to be successful, and we are in, as I said, serious jeopardy at the current amounts marked up, particularly coming on the heels of a major reduction for us in fiscal year 2005.

Another key issue, of course, is the issue of privacy, and, as I have said from the moment I assumed responsibility for this program, privacy and security are the two goalposts of Secure Flight. We have tried to design the system with privacy at its very core, and, as you know, we are undergoing very close consultations with GAO as well as the Privacy Officer at the Department, and we determined several weeks ago that the documents that we had issued to govern testing, which of course will be scrapped and renewed for the implementation of the program, did not adequately and fully reflect everything we had done during testing.

And so we took the initiative on our accord to amend those documents publicly, which we published a week ago today, to more fully explain what we have been doing. Of course, everything that is in those documents we have briefed extensively to the committee, others in the Congress and to GAO and the public, so it was a matter of making sure that our documents were aligned.

In addition to that, the Deputy Secretary has directed the Privacy Officer to conduct a review of all aspects of privacy in Secure Flight. We of course welcome that. We are working with the Privacy Officer on a daily basis, and so this is just more useful support for the program, and we are appreciative of that.

With respect to GAO's overall effort, which I know is of great interest to the committee, there are 10 separate criteria regarding Secure Flight that the Congress has directed GAO to review. GAO issued a preliminary report in March describing our progress in all 10 areas, and in that report included 6 recommendations, all of which we concur with, all of which were in progress at the time of publication and all of which we are nearing completion on. And we intend to meet all 10 GAO criteria before we start the program. That is our objective. Those criteria are things that we would normally do anyway, and so we are appreciative of that.

And then the final issue, of course, deals with redress, which has been a great topic of conversation today. I think Secure Flight of-

fers significant improvements in terms of how people who are particularly close matches to the list can navigate through the system much more efficiently than they do today. And I will be happy to discuss that in more detail.

So I really do appreciate the opportunity to testify. This is a very important program. We need to be talking with the American people as often as we can about what we are doing, because it is so broad based, and I look forward to your questions and questions from other members of the committee.

[The statement of Mr. Oberman follows:]

PREPARED STATEMENT OF JUSTIN P. OBERMAN

Good morning Mr. Chairman, Congresswoman Sanchez, and Members of the Subcommittee. I am pleased to have this opportunity to appear before you today on behalf of the Transportation Security Administration (TSA) to discuss our efforts and challenges relating to improving pre-screening of aviation passengers against terrorist and other watch lists, particularly in the context of our Secure Flight Program. The Department of Homeland Security (DHS) and TSA are committed to the development of Secure Flight as an essential layer in our system of systems approach to aviation security. We envision Secure Flight as a unique opportunity to leverage technology and information management practices to implement a program that enhances the security of the civil aviation system. An additional benefit of Secure Flight is the prospect for improving and facilitating travel for the broad public. We are working to quickly resolve remaining policy, technical, cost, and privacy considerations.

BACKGROUND

Currently, aircraft operators are required to compare the name of each passenger to the names of individuals on two Federal Government watch lists known as the No-Fly and Selectee Lists. When an aircraft operator has a reservation from a passenger with a name that is the same as, or similar to, a name on the No-Fly list, the aircraft operator is required to notify law enforcement personnel and TSA to verify whether that passenger is in fact the individual whose name is on either list. If the passenger is verified as an individual on the No-Fly List, the aircraft operator is prohibited from transporting the passenger and all accompanying passengers. When an aircraft operator has a reservation from a passenger with a name that is on the Selectee List, the aircraft operator is required to identify the individual to TSA for enhanced screening at security screening checkpoints.

In addition, domestic air carriers perform passenger pre-screening through their use of the Computer-Assisted Passenger Prescreening System (CAPPS). CAPPS, which was developed jointly by the airlines and the Federal government in the mid-1990s, analyzes information in passenger name records (PNRs) using certain evaluation criteria to determine whether a passenger and his property should receive a higher level of security screening prior to boarding an aircraft.

As part of the Aviation and Transportation Security Act (ATSA) (P.L. 107–71), Congress directed that the Secretary of Transportation ensure that "the Computer-Assisted Passenger Prescreening System, or any successor system—is used to evaluate all passengers before they board an aircraft; and includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened." This requirement became part of the mission of TSA, with overall responsibility transferring with TSA to DHS on March 1, 2003, as provided for in the Homeland Security Act of 2002 (P.L. 107–296).

The need to expedite implementation of an effective passenger pre-screening system was reinforced and reemphasized in the final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), which states at page 392:

> "[I]mproved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by TSA and it should utilize the larger set of watch lists maintained by the Federal Government. Air carriers should be required to supply the information needed to test and implement this new system."

Spurred by the recommendations of the 9/11 Commission, Congress enacted in relevant part Section 4012 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)(P.L. 108–458). The provision directs that TSA commence testing of and ultimately assume responsibility for "the passenger prescreening function of

comparing passenger information to the automatic Selectee and No Fly lists [utilizing] all appropriate records in the consolidated and integrated terrorist watch lists maintained by the Federal Government in performing that function."

Secure Flight is TSA's program to move the existing watch list vetting process of domestic passengers from the air carriers into the Federal Government in order to make the process more effective, consistent, and efficient for the traveling public from a security and customer service standpoint. Under this program, TSA will assume the function of conducting pre-flight comparisons of domestic passenger information to Federal Government watch lists, to include expanded versions of the No-Fly and Selectee Lists. TSA is also reviewing whether the Secure Flight system may be able to incorporate a streamlined version of the existing CAPPS system to evaluate information in PNRs that passengers otherwise provide to aircraft operators in the normal course of business.

BRIEF OVERVIEW OF SECURE FLIGHT'S GOALS

The importance of an effective Secure Flight program is hard to overstate. Because the airlines have varying systems by which they implement passenger prescreening, the effectiveness, efficiency, and consistency in response for airline passengers of the current system is limited. In developing Secure Flight, TSA is seeking that greater effectiveness, efficiency and consistency, but doing so requires the consolidation of functions that are now being carried out separately by 65 air carriers, for 1.8 million passengers on 30,000 flights fly each day, at approximately 450 airports where security screening is required. Once implemented, however, Secure Flight would enable TSA to better focus its resources and security screening efforts on those passengers who are identified to be more likely to pose a threat to aviation security. In addition to resulting in a more secure system, the benefits to legitimate travelers, who comprise the vast majority of the traveling public, will be evident. TSA fully appreciates the frustration felt by individuals posing no threat to aviation security who are selected for additional scrutiny at airports because of a false positive report that they match or resemble a name on a watch list. Once operational, Secure Flight will result in fewer individuals undergoing additional scrutiny, thus reducing one element of the "hassle factor." Furthermore, by reducing false positives, additional passengers will be able to avail themselves of expedited check-in procedures on the Internet and at self service ticket kiosks. The overall result would be a more secure system that is also more efficient and user-friendly to travelers.

In assuming the watch list checking role from the air carriers, we recognize that they are indispensable partners, without whom the Secure Flight program will not succeed. The carriers have been extremely cooperative, for example, in providing the necessary historic PNR data relating to domestic flights in June, 2004 to enable TSA to conduct its preliminary testing, and we expect that this cooperation will continue as we make preparations for beginning operational testing of Secure Flight. We are also partnering with U.S. Customs and Border Protection (CBP) on the transmission of passenger data because most domestic carriers already have pre-existing information technology connections to CBP relating to passenger data.

TSA also acknowledges that carriers are concerned with not only the technical issues relating to connectivity but also with the initial start-up costs that they might have to bear. TSA will continue to work with the airline industry to develop cost estimates for implementation and continued operations and is committed to working with the carriers in managing the start-up costs of Secure Flight, including the costs associated with aligning the IT systems. However, ultimately, the anticipated economies of scale that will be achieved by consolidating the watch list vetting function into the government, a function whose attendant costs are currently borne by the carriers, will likely lead to significant savings to the carriers. An additional benefit of Secure Flight is that the increased efficiency that it will afford at checkpoints and ticket counters should assist carriers in maintaining and improving passenger satisfaction and customer service—objectives that we share with the carriers as TSA carries out its primary mission of ensuring civil aviation security.

TERRORIST WATCH LISTS AND FUNCTIONALITY OF SECURE FLIGHT

Before I discuss further our efforts to develop and test Secure Flight and the issues that must be resolved prior to its actual deployment, please allow me to provide some information regarding the underlying terrorist databases on which passenger information will be compared. Homeland Security Presidential Directive 6 (HSPD–6) and an accompanying Memorandum of Understanding (MOU) dated September 16, 2003, directed the creation of the Terrorist Screening Center (TSC) and reengineered the terrorist watch list process.

Since its creation on December 1, 2003, TSC has developed and maintained the Federal government's Terrorist Screening Database (TSDB). TSDB receives inter-

national terrorist-related identity data from the National Counterterrorism Center (NCTC), also created under HSPD–6, and purely domestic terrorist information from the FBI. The NCTC receives nominations from U.S. Government agencies, such as CIA and FBI, for placement on specific Federal watch lists. The NCTC then creates records in its terrorist identities database and forwards the originator nomination to the TSC. The TSC then provides unclassified identity data to TSA for use in its No-Fly and Selectee lists, based on specific No-Fly and Selectee nominations from agencies. TSA personnel at the TSC provide quality assurance and monitor the transmission of this data.

Currently, TSA's role is to provide the No Fly and Selectee lists to foreign and domestic air carriers that service U.S. airports. TSA has provided the air carriers with guidance on how to handle and operate the lists via Security Directives and Emergency Amendments, and TSA's 24x7 watch centers take air carrier reports and coordinate No-Fly and Selectee operational issues. TSA continues to work closely with TSC to ensure as much as possible that the watch lists are accurate and comprehensive. Additionally, TSA maintains a list of cleared individuals whose names are similar to those contained in the watch lists. Cleared lists with identifying information are attached to the No Fly and Selectee lists to assist carriers in distinguishing between watch listed and non-watch listed passengers.

Secure Flight will involve the comparison of passenger information for domestic flights to names in the TSDB maintained by the TSC, including the TSA No-Fly and Selectee Lists, to identify individuals known or suspected to be engaged in terrorist activity. Secure Flight will automate the vast majority of watch list comparisons, will allow TSA to apply more consistent procedures where automated resolution of potential matches is presently not possible (due to the current reliance on separate procedures at each airline), and will allow for more consistent response procedures at airports for those passengers identified as potential matches.

Bringing the watch list matching function into the Federal government will also permit expansion of these lists to include sensitive information that could not be disclosed to the airlines. Under the current system, TSA has great concerns over the security aspects of providing air carriers and many of their employees with information contained on the No-Fly and Selectee Lists. These security concerns would be reduced once the Federal government assumes the responsibility for administering watch list comparisons, thus permitting integration and consolidation by TSC of additional information relating to individuals known or suspected to be engaged in terrorist activity.

PROGRESS AND CHALLENGES

On September 24, 2004, TSA published in the *Federal Register* a number of documents necessary to allow the agency to begin testing the Secure Flight program. These included: (1) a proposed order to U.S. aircraft operators directing them to provide a limited set of historical passenger name records (PNRs) to TSA for use in testing the program (69 FR 57342); (2) a Privacy Act System of Records Notice (SORN) for records involved in testing the program (69 FR 57345); and (3) a Privacy Impact Assessment (PIA) of program testing (69 FR 57352). These documents explained that in addition to testing TSA's ability to conduct automated watch list comparisons for purposes of the Secure Flight program, TSA intended to conduct a separate test to determine whether the use of commercial data would be effective in identifying passenger information that is incorrect or inaccurate. TSA updated the SORN and PIA on June 22, 2005 (70 FR 36320).

On November 15, 2004, TSA published in the *Federal Register* a document setting forth, among other things: TSA's response to public comments on the September 24, 2004, proposed order; revisions made to the proposed order in response to comments; and the text of the final order. (69 FR 65619). The final order directed U.S. aircraft operators to provide to TSA, by November 23, 2004, a limited set of historical PNRs for testing of the Secure Flight program.

Utilizing the data provided by air carriers, TSA commenced testing of the watch list matching function for Secure Flight beginning in November, 2004. The testing involved 15 million PNRs relating to flights flown domestically on every U.S. carrier in June, 2004. That test demonstrated that the system was effective in matching PNR data with data contained in terrorist watch lists and that the system can handle the expected load of more than 1.8 million passengers per day. The preliminary testing also enabled TSA to determine that it must obtain, at a minimum, an individual's full name and date of birth in order to perform an effective comparison of that individual against those individuals identified on the No-Fly and Selectee Lists. Testing showed that use of date of birth is helpful in distinguishing a passenger from an individual on a Federal watch list with the same or similar name and significantly reduced the number of false positive watch list matches.

In addition to the testing to determine TSA's ability to compare passenger information with data maintained by TSC, TSA is continuing with a separate set of testing involving commercial data. Our purpose is to test the Government's ability to verify the identities of passengers using commercial data and to improve the efficacy of watch list comparisons by making passenger information more complete and accurate using commercial data. In conducting commercial data testing, procedures have been put in place to ensure strict adherence by contractors and their personnel to privacy standards and data security protections. No decision has yet been made on whether commercial data will ultimately be used in Secure Flight. If TSA decides to use commercial data for Secure Flight, it will not do so until the agency publishes a new SORN and PIA announcing how commercial data will be used and how individuals' privacy will be protected. TSA will not be using commercial data upon the initial rollout of Secure Flight.

Let me say a bit more about the importance TSA gives to incorporating privacy rights protections in the design of Secure Flight. The protection of privacy is an omnipresent concern as TSA tests, develops, and implements Secure Flight. We are resolute in our commitment to adhere to the letter and intent of the Privacy Act and applicable policies on privacy protection and are endeavoring to resolve all of the outstanding issues relating to privacy. Moreover, we have continuously consulted with various privacy advocates to seek best practices and share details about this important program, and we will continue to work with the DHS Privacy Officer on the privacy issues relating to Secure Flight.

As you are probably aware, recently, the Deputy Secretary requested the Department's Privacy Officer to assess the handling of PNR information and commercial data during the testing phase and to provide any recommendations about how to strengthen our focus on privacy protection as we continue testing and contemplate deployment of Secure Flight. The Deputy Secretary has made the same request of the Department's new Data Privacy and Integrity Advisory Committee. I met with this group in Boston last week to brief them and to solicit their counsel. Throughout our testing of commercial data, Government Accountability Office (GAO) and interested committees in Congress have been made fully aware of the details surrounding our goals and methodology in conducting this testing.

On June 22, 2005, TSA amended the scope of the SORN and PIA to clarify and describe with greater particularity the categories of records and categories of individuals covered by the Secure Flight Test Records system. The GAO also has conducted extensive assessments of Secure Flight, including recently our use of commercial data testing. TSA is cooperating fully to ensure that all privacy concerns are addressed in an appropriate manner.

TSA has employed data security controls, developed with the TSA Privacy Officer, to protect the data used for Secure Flight testing activities. The procedures and policies that are in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses. Measures that are in place include the following:

- Access to private information is limited to only those TSA employees and contractors who have a "need to know" to perform their duties associated with Secure Flight operations;
- A real-time auditing function is part of this record system to track all whoaccesses information resident on electronic systems during testing, and all instances when records are transmitted between TSA and contractors are meticulously kept;
- Data is maintained at a secure facility, and the information is protected in accordance with rules and policies established by both TSA and DHS for automated systems and for hard copy storage, including password protection and secure file cabinets;
- Each employee and contractor associated with the Secure Flight program has completed mandatory privacy training prior to beginning work on the program.

Many technical challenges remain as TSA continues its work on testing Secure Flight in preparation for implementation and deployment. To ensure that these hurdles are overcome, it is absolutely necessary that Congress fully support the request in the President's budget for FY06, which proposes that Secure Flight be funded at $81 million. I would emphasize that if the program is ultimately funded at levels comparable to the $66 million or $56 million in the bills that have been approved by the House and reported in the Senate that a delay in implementation will be unavoidable.

TSA recognizes the importance of having in place a redress system that is readily available to passengers. TSA has already developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A

passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA reviews the submission and reaches a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. It is important to emphasize, however, that this clearance process is distinct from the ongoing internal review process to ensure that persons do not remain on the watch lists if they are found not to pose a security threat. TSA's clearance process distinguishes passengers who are not a security concern from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

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.

In addition to the mandates of IRTPA, Section 522 of the Homeland Security Appropriations Act, 2005 (P.L. 108–334) requires TSA to satisfy and GAO to report that TSA has addressed ten areas of Congressional interest relating to the Secure Flight program. On March 28, 2005, GAO released a report concluding that while "TSA has not yet completed these efforts or fully addressed these areas, due largely to the current stage of the system's development", "TSA is making progress in addressing each of the key areas." GAO also issued six recommendations to assist TSA in managing the risks associated with the implementation of the Secure Flight program:

1. Finalize the system requirements document and the concept of operations, and develop detailed test plans—establishing measures of performance to be tested—to help ensure that all Secure Flight system functionality is properly tested and evaluated. These system documents should address all system functionality and include system stress test requirements.
2. Develop a plan for establishing connectivity among the air carriers, CBP, and the TSA to help ensure the secure, effective, and timely transmission of data for use in Secure Flight operations.
3. Develop reliable life-cycle cost estimates and expenditure plans for Secure Flight—in accordance with guidance issued by the Office of Management and Budget—to provide program managers and oversight officials with information needed to make informed decisions regarding program development and resource allocations.
4. Develop results-oriented performance goals and measures to evaluate the effectiveness of Secure Flight in achieving intended results in an operational environment—as outlined in the Government Performance and Results Act—including measures to assess associated impacts on aviation security.
5. Prior to achieving initial operational capability, finalize policies and issue associated documentation specifying how the Secure Flight program will protect personal privacy, including addressing how the program will comply with the requirements of the Privacy Act of 1974 and related legislation.
6. Prior to achieving initial operational capability, finalize policies and procedures detailing the Secure Flight passenger redress process, including defining the appeal rights of passengers and their ability to access and correct personal data.

TSA has systematically proceeded within the framework outlined by GAO to address the ten areas of Congressional interest identified in P.L. 108–334. With regard to the fifth recommendation, TSA is absolutely committed to safeguarding personal privacy and to complying with the letter and intent of the Privacy Act of 1974. As I previously discussed, many safeguards are already in place, and as we learn more through our ongoing testing, we will devise and implement the appropriate measures and will be updating the associated documentation as illustrated by our actions last week in issuing a revised SORN and PIA.

CONCLUSION

The implementation of an improved program for pre-screening of passengers against watch lists, as identified by the 9/11 Commission and Congress, is a vitally important mission and is a high priority for TSA and the Department. We appreciate the support that you have voiced for expeditious implementation of Secure Flight and your recognition of the program's great potential for further improving aviation security. We acknowledge the concerns over our progress in development of the program and other related issues and are heavily engaged in resolving issues of concern. We will continue to work with you and other interested Members and Committees in Congress on Secure Flight and will keep you apprised of important developments as they occur.

Mr. Chairman, Congresswoman Sanchez, and other Members of the Subcommittee, this concludes my prepared remarks. I would be pleased at this time to answer any questions.

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

I recognize myself for 5 minutes of questions.

First of all, if you could describe the Secure Flight Program and how it would improve, if at all, the question that was raised by Mr. Anderson's experience and the one related by the Ranking Member of the person in her district, as well as Ms. Lofgren's husband. How will the mechanics of the Secure Flight Program in any way impact those situations?

Mr. OBERMAN. They will positively impact them in several different ways, which I would be happy to describe.

Mr. LUNGREN. Okay. Maybe you need to sort of describe the program and then show how this would specifically affect that.

Mr. OBERMAN. Absolutely. Firstly, we are going to require passengers to provide us with their full name and their date of birth when they travel. The reason for that is twofold: Number one, most of the records in the watch list contain name and a date of birth, and then the data elements that are there significantly drop off. And that is because we do not have perfect information on terrorist threats by virtue of the fact that they are terrorist threats, not making themselves visible.

So by having a full name and date of birth, we will be able to resolve a significant number of close matches before the person ever arrives at the airport at all. And our testing has shown that we can reduce that false-positive rate by at least 60 percent.

Secondly, we will be the only—

Mr. LUNGREN. Is that because you will have the date of birth?

Mr. OBERMAN. That is right.

Mr. LUNGREN. Which is an identifier you do not have now?

Mr. OBERMAN. That is correct.

Mr. LUNGREN. And when you say, "full name," does that include middle initial, middle name?

Mr. OBERMAN. Yes, it does. It is the name that you present on your travel documents, for example, your driver's license, which we also do not have in every passenger record today.

Mr. LUNGREN. Thank you.

Mr. OBERMAN. The second thing that will be different under Secure Flight and also will help mitigate the difficulties that people such as Congressman Anderson are having is the fact that we will be the only entity responsible for vetting. There are 65 carriers in the United States, all of whom do this process slightly differently from one another, leading to inconsistencies like the one that Congresswoman Sanchez described with a passenger on a specific air-

line having trouble and then on another carrier, another day not having the same kind of difficulty.

As a result of our being able to be the only vetting entity and the fact that this is a core function for TSA, not a core function for an airline, we will have state-of-the-art technology to do name matching. That is not what the air carriers use today. We have the best available, and we are continuing to partner with the Terrorist Screening Center and others to make sure that we have state-of-the-art technology, much greater accuracy in terms of matching.

The third thing is, we are going to have a team of very experienced intelligence analysts looking at all of these close matches and making judgments about whether somebody is in fact on the list. The carriers do an excellent job of this today by necessity so they can keep their system operating, but our folks are trained to do this and have been doing it in almost every case since before 9/11.

Finally, we will be the only entity applying these so-called cleared lists of people who were never on the list in the first place, went through our redress process and received relief, for example, Congressman Anderson who is now on the cleared list. Again, we will not have 65 separate airlines running that list differently, and we will also have a new redress office, triple the staff that is there today, with new procedures. It is going to be far better than?

Mr. LUNGREN. So right now, if you clear Mr. Anderson, you then give notice to all the airlines of that, correct?

Mr. OBERMAN. That is right.

Mr. LUNGREN. And then you have to rely on however they operate their systems.

Mr. OBERMAN. That is correct.

Mr. LUNGREN. And under the Secure Flight Program, you will no longer put that responsibility on the airlines, it will be your responsibility solely.

Mr. OBERMAN. That is correct.

Mr. LUNGREN. Let me ask you with respect to the question of commercial databases, you have said that with the additional information of the full name and the date of birth, that will eliminate 60 percent of the names, correct?

Mr. OBERMAN. Sixty percent of the close matches, that is correct.

Mr. LUNGREN. Of the close matches, yes. So then you are still dealing with 40 percent. Obviously, you have got more names on there than there are people that you want to keep off the airplane or more people that you are checking against then. How do you then go through that second analysis and what bits of information or data do you need for that?

Mr. OBERMAN. Couple different things that we are going to do under Secure Flight. Firstly, as I said, we will have a team of very experienced analysts take a look at Bob Lewis flying out of LAX on a particular day, which now will be given to us as Robert M. Lewis with a date of birth. So it may not be flagged in the first place, but if he still is, we will have a team of experienced analysts with access to underlying classified information, supports the watch list record, to be able to make a determination.

In addition to that, one of the things that we have tested over the last 4 or 5 months, which we are still doing the testing, it is not conclusive enough yet to be able to make a judgment, is looking

at whether bringing additional information into that passenger's record, for example, their address, their phone number, things of that nature would enable us to further distinguish it.

Comments Mr. Rosenzweig made about dates of birth and zip codes being very good identifiers is precisely one of the things we have been looking at, and we have not been pulling in just the street address but also the zip code to make a differentiation. And that is one potential benefit of using commercial data, which is the subject of a test and ongoing work to see if it will be effective.

Mr. LUNGREN. My time has expired.

The Ranking Member of the full committee, Mr. Thompson, is recognized for 5 minutes.

Mr. THOMPSON. Thank you very much.

Let me welcome you, Mr. Oberman, to the committee.

There are a couple of questions I would like to get answered in my mind about Secure Flight. Would Secure Flight pick up a person with strong community roots but who is in a terrorist sleeper cell or would a person have to be a known terrorist in order for Secure Flight to pick him up?

Mr. OBERMAN. Let me answer that this way: It will identify people who are known or suspected terrorists contained in the terrorist screening database, and it ought to be able to identify people who may not be on the watch list. It ought to be able to do that. We are not in a position today to say that it does, but we think it is absolutely critical that it be able to do that.

And so we are conducting this test of commercially available data to get at that exact issue. Very difficult to do, generally. It is particularly difficult to do when you have a system that transports 1.8 million people a day on 30,000 flights at 450 airports. That is a very high bar to get over.

It is also very difficult to do with a threat described just like you described it, which is somebody who has sort of burrowed themselves into society and is not readily apparent to us when they are walking through the airport. And so I cannot stress enough how important we think it is that it be able to have that functionality. And that is precisely the reason we have been conducting this commercial data test, why we have extended the testing period and why we are very hopeful that the results will prove fruitful to us so that we can then come up here, brief them to you and explain to you why we need to include that in the system.

Mr. THOMPSON. Well, since we have used Mr. Anderson as our person, what happens if a terrorist is traveling on stolen identity? How can this system pick that person up?

Mr. OBERMAN. Again, it is a critical threat area that we are worried about and something that we are hopeful that the use of commercial data will be able to address. Right now if we take the names of passengers as they are provided to the carriers and we compare them to the watch list, we will generate matches.

It happens dozens of times a day across the country in all modes of transportation, including aviation, today. That is a terrorist giving us an identity that is known to the government. But, as I said, it will not be adequate for an aviation pre-screening system in the United States if it relies only on information provided by the passenger. We do not think that is enough.

And so the purpose of testing the use of commercial data is to see if we can attain that functionality. As I said, it is a very high bar to get over because of the complexities of our system, but we think it is just fundamental to our overall mission to secure the aviation system in the United States.

Mr. THOMPSON. And I will follow up that line of questions, Mr. Chairman, with some additional questions for our witness, but I want to go to another point.

It is my understanding that Carol DiBattiste, formerly of TSA, has been hired as ChoicePoint's chief privacy officer. Are you aware of that?

Mr. OBERMAN. Yes.

Mr. THOMPSON. But I am also told that there was a point in time that a contract had been offered to ChoicePoint through EagleForce Associates. Are you aware of any of this information?

Mr. OBERMAN. It is not correct, Congressman. EagleForce is conducting a commercial data test on behalf of TSA and has contracted with three separate commercial data providers.

Mr. THOMPSON. Is ChoicePoint one of them?

Mr. OBERMAN. ChoicePoint is not one of them.

Mr. THOMPSON. So ChoicePoint is not involved in it at all.

Mr. OBERMAN. That is correct.

Mr. THOMPSON. Well, I am glad to know that. Now, I have a letter that I sent to the Department in March of this year which has yet to be responded to. I will provide you with another copy of that letter in hopes of within the next 10 days we can get it responded to.

Mr. OBERMAN. We will get it up here quicker than that.

[Information follows:]

One Hundred Ninth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

March 17, 2005

The Honorable David M. Stone
Director
Transportation Security Administration
U.S. Department of Homeland Security
701 12th St., West Tower
Arlington, VA 22202

Dear Admiral Stone:

According to recent reports, the Deputy Administrator of the Transportation Security Administration (TSA), Carol A. DiBattiste, has accepted a position with ChoicePoint to begin on May 2, 2005. Recently, TSA awarded a $475,000 contract to test the use of commercial data for Secure Flight to EagleForce Associates, which announced it is hiring ChoicePoint as its major subcontractor. This turn of events raises a number of questions that I request you answer:

1. What role did Ms. DiBattiste have in the review or evaluation of EagleForce Associates' contract proposal for the Secure Flight program or any other contracts that EagleForce Associates has received from TSA?

2. Did EagleForce Associates' contract proposal discuss its plans to subcontract with ChoicePoint?

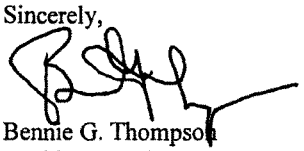
3. Has Ms. DiBattiste played any role whatsoever in the review or evaluation of any of ChoicePoint's contract proposals?

4. Did Ms. DiBattiste discuss potential employment opportunities with ChoicePoint during the time that EagleForce Associates' proposal was under consideration?

Additionally, I would appreciate receiving copies of the response to any Freedom of Information Act requests you have received related to Ms. DiBattiste's relationship with EagleForce Associates or ChoicePoint.

If you have any questions about this letter, please contact Todd Gee on the Democratic staff of the House Committee on Homeland Secuirty at (202) 226-2616.

Sincerely,



Bennie G. Thompson
Ranking Member
House Committee on Homeland Security

Office of the Assistant Secretary
U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

MAR 25 2005

Transportation Security Administration

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Thompson:

Thank you for your letter of March 17, 2005, regarding the recent award to EagleForce Associates (EagleForce) for commercial data testing on the Secure Flight program. You asked a series of questions concerning this award to EagleForce, and the media reports of the selection of ChoicePoint as its major subcontractor. In particular, you asked about the involvement of the Transportation Security Administration (TSA) Deputy Administrator, Carol DiBattiste, in the award of this contract to EagleForce.

In reviewing the facts, we have learned that EagleForce has, in fact, not issued a subcontract for the Secure Flight testing to ChoicePoint. Also, Ms. DiBattiste did not participate in the selection of EagleForce for commercial data testing for Secure Flight. We have seen press statements, including a Congressional Quarterly article, reporting that "...EagleForce plans to hire ChoicePoint, DiBattiste's new employer, as the major subcontractor." These statements, however, are not correct. Specific answers to your questions are provided below:

1. Ms. DiBattiste played no role in the review and evaluation of any proposal associated with the Secure Flight commercial data testing.
2. ChoicePoint is not a subcontractor to EagleForce. In its proposal, EagleForce indicated that it had identified a number of commercial data sources available to perform testing. It listed ChoicePoint as a potential source, along with nine other potential sources. EagleForce later selected three commercial data providers for the testing. ChoicePoint is not one of the selected providers.
3. Ms. DiBattiste has not played any role in the review and evaluation of ChoicePoint contract proposals. TSA has awarded only one contract to ChoicePoint in August of 2003, and she was not involved in the proposal review, evaluation, or selection.
4. Ms. DiBattiste recused herself from participating in any particular matter that could affect the financial interests of ChoicePoint when she commenced employment negotiations with that company on February 6, 2005. The contract for EagleForce was awarded on February 22, 2005.

Further, to date TSA has not received any Freedom of Information Act requests regarding Ms. DiBattiste's relationship with EagleForce or ChoicePoint.

I hope that this information is helpful. If your staff needs further information or assistance, they are requested to call Mr. Peter A. Iovino, Director, Office of Legislative Affairs, at (571) 227-2717.

Sincerely yours,

David M. Stone
Assistant Secretary

Mr. THOMPSON. Thank you, Mr. Chairman.

Mr. LUNGREN. The gentleman from California, Mr. Cox, is recognized for 5 minutes.

Mr. COX. Thank you, Mr. Chairman.

I am sure you were here for the first panel and saw all that testimony, and everyone has to be very sympathetic with the plight of John B. Anderson. At least all of us in Congress know who John B. Anderson is and the fact that not only was he a member of the House of Representatives but a pretty well known at the time candidate for President of the United States.

Do you believe that what happened to him when he tried to fly to Germany with formers Members of Congress is likely to happen again if he chooses a different carrier next time?

Mr. OBERMAN. I do not know, and the reason is every airline applies this cleared list in a slightly different manner.

Mr. COX. So since you do not know, the answer is it could happen again.

Mr. OBERMAN. Yes, it could.

Mr. COX. What can we do to make sure that it does not or to ask the question more broadly, what can we do to make sure that this system learns? My understanding is that we have thousands of false matches every day and that a lot of John Andersons exist and these people then are going to extraordinary lengths to educate the system, at least in connection with their upcoming trip about why they are not the person that the system thinks they are. Having gone to those lengths, doesn't the traveler deserve to just do it that once?

Mr. OBERMAN. We need to fully fund Secure Flight so that we can put in place a system—

Mr. COX. Yes, and I am all for Secure Flight, I hope it happens, but we have got a system in place right now.

Mr. OBERMAN. Yes.

Mr. COX. Are you saying that it is absolutely incapable of learning?

Mr. OBERMAN. I am not saying it is incapable of learning, but the issue is that the carriers are not as a matter of their first priority in the watch list checking business. And when we put someone on a cleared list, it is the same mechanics of checking names of people who are flying against names on a cleared list. And the problem is—

Mr. COX. But why do we have to keep doing it over and over and over again the same way so that the system does not learn anything? Every time that I show up at the airport, even if I have been there many, many times, the system thinks it is my first time.

Mr. OBERMAN. Yes. The answer is that some carriers are working right now before Secure Flight is up and running on systems that I do not think remember is necessarily the priority, it is more that we can differentiate and know that this particular John B. Anderson is the former Member of Congress and presidential candidate and not the person that is on the watch list. And they are using other identifiers.

Now, they do not have the date of birth currently, so some carriers are working on systems which, for example, the would use the frequent flyer number. But it is the same premise that we are try-

ing to get to under Secure Flight, which is to have additional identifiers to distinguish these passengers.

And the issue is, from a TSA standpoint and I think also from a congressional standpoint, it is a matter of coaxing and urging and consulting with the air carriers to help them get there in what is admittedly a very difficult financial environment, while we are also asking them to make changes to their system to comply with Secure Flight.

But I am aware of some carriers now who are trying to make their systems smarter so that they can distinguish between the John B. Anderson who may or may not have flown the day before but is already on the cleared list and the John B. Anderson that may in fact be on the terrorist watch list, and other identifiers are the way that they are doing it.

Mr. COX. So we are just leaving it to every air carrier to do their own thing and the TSA is not going to fix this problem.

Mr. OBERMAN. TSA is not in a position under the current system to fix it in the way that you are describing, and that is because we issue security directives that require the carriers to use these lists. We have some specific requirements as to how they are supposed to run those lists, but that security directive does not come with a software package.

Mr. COX. You know, what happens then as a result is that the federal government, TSA included, is spending a whole lot of money looking at the wrong people. To the extent that we are looking at John B. Anderson as he goes again through the airport, definitionally we are wasting resources that should be focused on potential terrorists. So the fact that our system in incapable of learning is not only diverting our attention away from actual counterterrorism but it is wasting resources and taking us a step backwards. Those resources should be applied to finding real terrorists.

The main job here since we are dealing with the domestic U.S. population has to be to reduce the size of the haystack. By and large, we can rest assured that 300 million Americans are not a problem and yet our system right now seems intent on increasingly drilling down into the population that we know is not the problem.

In my own case, just in this town, with the same zip code, there is Chris Cox over at the White House and Legislative Affairs responsible for homeland security. There is Chris Cox who runs the NRA. My first name is Charles. There is a Charles Cox who in the Reagan administration was a Commissioner of the Securities and Exchange Commission.

None of these people is me, but if we have a name-based system, we are going to make it very, very difficult on ourselves. We are going to make it a big time waster and a resource consumer when the real job is to look for terrorists who in the main are overseas people.

The software that we are using of the National Tracking Center for international flights, trying to match passengers to lists, I was advised, worked an awful lot better with Anglo-sized names than it does with foreign names. This name approach that we have got is not anywhere near to a system of unique identifiers that we are going to need. And I do hope that we can quickly remember what—

get back to first principles and remember what this is supposed to be all about, which is finding terrorists.

Let me just ask one final question and that is about the problem of screening of infants, which the chairman raised. TSA's view is that is not supposed to happen. Indeed, I think your guidance is do not automatically shunned to secondary screening anyone under 12; is that right?

Mr. OBERMAN. Correct.

Mr. COX. Right now I cannot get a boarding pass in advance, I cannot print it out on my home computer or even at a kiosk, I do not believe, if I have been flagged for secondary screening according to the behavioral criteria; is that right?

Mr. OBERMAN. Right.

Mr. COX. So what happens is I have to show up at the airport, and if I have got an infant in tow then what should happen from TSA's standpoint so that we do not keep having baby John Andersons go through this process?

Mr. OBERMAN. Let me answer that, and I do want to just pick up on the other point you raised before the alarm there.

You are correct in your understanding of how the procedures are supposed to work, and we are making additional changes, which are not finalized yet at TSA, some of which are classified in nature so I cannot discuss them in detail here, to further mitigate that problem, to give us more discretion so that we can move people through the airport faster. We can brief you about that in a secure setting, but we are making changes in response to some of these issues, literally, in the imminent future.

Mr. COX. I am very happy to hear that.

Mr. OBERMAN. Okay. And then just with respect to the other issue, let me just make two points. I think, as I have said, you are starting to see the air carriers innovate to some extent. And, again, it is a very difficult environment for them to innovate given all the other challenges they face. And that is going to help this problem before we fully roll out Secure Flight. I think that is going to hopefully take off across the industry.

The second thing, though, is we are applying state-of-the-art technology at TSA to this problem, and you need two things. You need state-of-the-art technology, and so, you are right, CBP has the technology that is excellent, we are going to use that at the State Department the same way, the private sector as well, and we are going to put all that together and have a state-of-the-art matching system.

The second thing, though, is we need to be able to have unique identifiers into the system, and we agree that a name-based system is not adequate but we have to remember that the terrorist watch list starts with names, it goes to dates of birth and then the unique identifiers drop off. And so that is why Secure Flight will require full name and date of birth to mitigate so many of those false matches before the person ever gets to the airport.

Mr. COX. I am sorry, Mr. Oberman, just if you would answer the question about the baby John Anderson.

Mr. OBERMAN. That is going to be addressed in the procedural changes that we are making.

Mr. COX. Oh, you have to address that in the classified setting.

Mr. OBERMAN. That is correct.

Mr. COX. Thank you.

Mr. LUNGREN. Mr. Dicks is recognized for 5 minutes.

Mr. DICKS. Mr. Chairman, our staff put together a Secure Flight missed milestones. I just would like to put a copy of that in the record if that is possible.

Mr. LUNGREN. I do not think there is any problem.

Mr. DICKS. Let me just of forward. TSA is making progress—this is a GAO report—in the development and testing of Secure Flight and it attempting to build in more rigorous processes than those used for CAPPS II. Specifically, TSA has drafted a number of key documents to assist in providing program oversight, including a draft concept of operations, a draft requirements document and a draft project schedule. However, TSA has not yet finalized these documents.

Further, although TSA uses a working milestone chart to coordinate its many activities, key milestones for the Secure Flight Program have slipped. For example, the date when Secure Flight is expected to achieve initial operating capability with two air carriers slipped by about 4 months. TSA is also completing initial Secure Flight testing to determine data needs and system functions, which are basic to defining how Secure Flight will operate.

However, key systems testing, including stress testing to verify that the entire system will function as intended in an operational environment, has not been completed, and we are now July almost.

Further, although TSA expects to complete stress testing prior to initial operational development scheduled for August 2005, it has not yet designed the procedures that we will use to conduct these tests.

Until TSA finalizes key program documents and completes additional system testing, it is uncertain whether Secure Flight will perform as intended and whether it will be ready for initial operational deployment by August of 2005. What do you have to say about that? Is that all true? Is all that accurate?

Mr. OBERMAN. No. Here is what I have to say, a few things. Firstly, several of those documents have subsequently been completed since the GAO report was issued in March, and we, as you know, have turned over hundreds of thousands of pages of documents and continue to do it on a daily basis with GAO. The concept of operations is done, for example.

The second thing is we are in very serious jeopardy of missing our planned dates, because we do not have the funding we need to turn the program on.

Mr. DICKS. Okay. Explain that.

Mr. OBERMAN. Okay. I would be happy to.

Mr. DICKS. Congress cut the money?

Mr. OBERMAN. Yes.

Mr. DICKS. How much did they cut?

Mr. OBERMAN. In 2005, the President requested $60 million; we got $35 million. That is a 40 percent cut. In 2006, the President requested $81 million. The House mark is $66 million. That is a 20 percent cut. The Senate mark is $56 million. That is a 30 percent cut. We cannot make it go at those funding levels.

And the reason for that is several-fold. Firstly, it is very costly to test and develop a system of this complexity that has to connect to 65 air carriers and run more than 1.8 million transactions every day with no failure, including the day before Thanksgiving, Spring Break and so forth.

The second thing is the costs associated with connecting to each individual carrier—

Mr. DICKS. Is all that work being done by contractors?

Mr. OBERMAN. It is being done by contractors and federal employees together.

Mr. DICKS. Okay. Go ahead.

Mr. OBERMAN. Okay. And so it is important that the way we spend the money is understood. The costs associated with connecting each individual carrier because of the vagaries in their systems and the differences in the way that United might add the passenger's date of birth compared to how American might do it is very costly. Okay? So that is number one.

The second thing is the way we connect to an airline is a process that takes about 5 or 6 months per carrier, because a lot of that testing that GAO described has to be done once my regulation is issued, and I have got real—

Mr. DICKS. None of it has been done yet.

Mr. OBERMAN. A lot of testing has been done, and a lot of testing is still to be done.

Mr. DICKS. Stress testing?

Mr. OBERMAN. Yes, absolutely. We were able to run 2.7 million records in a 24-hour period. One point eight million people fly daily; we beat that stress test. We have to run 31 records a second. There are 28 records a second. We only run 31 records a second. All of our stress tests we met those thresholds, but that was with test data from June of 2004 that was historical and in a lab.

What GAO is referring to, which we fully concur with, is running a live test when I have actual passenger data coming in and I am really vetting it. That is considered a test and it has not begun yet, and what I cannot do is start the test, turn it off because I run out of money and try to turn it on again. It is a continuous incline to get every carrier connected. I am 40 percent sure in 2005, and I need the President's budget funded.

Mr. DICKS. Now, if you have the watch list, if you have the responsibility for doing the watch list, which you say you want, the Commission says you want, Congress has told you to do, you will have a better and more comprehensive list to use; isn't that correct?

Mr. OBERMAN. That is correct.

Mr. DICKS. Because one of the problems up to now is the lack of willingness of these intelligence agencies to share with the airline some of these names; isn't that true?

Mr. OBERMAN. Yes. I am not sure it is a lack of willingness. I think that there are real legitimate—

Mr. DICKS. Okay. Well, that means there is a lack of willingness.

Mr. OBERMAN. We will have a bigger and more comprehensive watch list for Secure Flight.

Mr. DICKS. So we should do better. You saw this story about the processing of passports in the New York Times today?

Mr. OBERMAN. Yes.

Mr. DICKS. I mean, that is pretty bad, isn't it? Doesn't that undermine your whole ability to do your job if passports are not properly issued?

Mr. OBERMAN. It does not undermine my ability to do my job in the sense that I am focused on domestic passengers, and if somebody uses their passport as their travel document and submits me their full name and date of birth, as required under Secure Flight, I am using the full terrorist screening database to flag that person.

Mr. DICKS. It says here, "The names of more than 30 fugitives, including 9 murder suspects and one person on the FBI investigations Most Wanted list did not trigger any warning in the test of the nation's passport processing system, federal auditors have found."

Mr. OBERMAN. I cannot speak to the details of that, because I am not responsible for the testing or administration of that. I just cannot speak to those specific details about those records and the names that were cleared.

Mr. DICKS. Well, let me just say what they tell you. I think it is important for you to know. Maybe you can talk to Mr. Moss. We are certainly going to do that, I hope. The lapses occurred because passport applications are not routinely checked against comprehensive lists of wanted criminals and suspected terrorists, according to the report, which was provided to the New York Times by an official critical of the State Department who has access to it in advance. For example, of the 67 suspects included in the test managed to get a passport 17 months after he was first placed on the FBI wanted list, the report said. I mean, that is not acceptable.

Mr. OBERMAN. All I can say is that—

Mr. DICKS. And I see people out there at the airport using their passport as their document to identify themselves, so that has got to be a problem.

Mr. OBERMAN. All I can tell you is we have our hands full trying to get Secure Flight started. We are going to use the terrorist screening database of known or suspected terrorists from boarding domestic flights of the United States. I am not in a position to speak to those details.

Mr. DICKS. All right. Thank you.

Thank you, Mr. Chairman.

Mr. LUNGREN. I hope it is not a sting program to bring them into the State Department.

The gentlelady from Texas, Ms. Jackson-Lee, is recognized for 5 minutes.

Ms. JACKSON-LEE. I thank you.

Thank the witness very much for his presence.

I understand one of my colleagues raised this and raised it earlier, but I will raise it with you again with respect to the watch list. I believe it would be appropriate to pose it to you. What information can you give on the value or the results of the utilization of the watch list in terms of deterring a tragic terrorist act, arresting a terrorist, getting information about terrorism or terrorist cells? What is it that we can secure that shows the validity of this watch list as it is presently constructed?

Mr. OBERMAN. I can discuss some of that. I think some of that information is more appropriate for classified setting, and I think much of that information is more appropriately provided by the Bureau and others.

What I can tell you is that—

JJACKSON-LEE. And if you would just yield for a moment.

Mr. Chairman, I would, Ranking Member, appreciate that we have an opportunity for a classified briefing on some of these questions so that we can both constructive and probative in our decision-making on this issue.

Mr. LUNGREN. I thank the gentlelady for her suggestion, and Mr. Oberman has suggested that he would be available for that in his prior testimony, and I am sure we are going to take him up on that.

Ms. JACKSON-LEE. I appreciate it very much. And let me just, if you can take this other question so that as you answer, you can answer this as well.

The enormous problem that we have is also a privacy question that we are all concerned about. I note on September 21, 2004, TSA released Privacy Act notices for the Secure Flight data. These notices included a privacy impact assessment, system of records notice, et cetera. In the notice, TSA claimed several exemptions from Privacy Act requirements for the test. On June 22, TSA issued a revised privacy notice for Secure Flight that amends the scope of the system and clarifies and describes with greater particularity the categories of records and categories of individuals.

Can you explain that dilemma or that different step? Can you also explain, as you answer this other question, this whole issue of behavior that the airlines use, and I consider it ineffective and whether it should be under their jurisdiction.

And my last point is the training, which is off the point, but I just simply hope you convey this. We need to work with TSA and the training of your airline screeners. I just want to go on record on that. You have a deficit in the training and the style and the appropriateness. You have hardworking individuals there, let me acknowledge that on the record, but you have got a deficit, as I travel and many of my constituents travel, in the treatment that these individuals provide. We would like them to be the first-line defense, but we do not like them to attack a grandmother, suggesting that that person is a terrorist and their treatment acts accordingly.

I yield to the gentleman.

Mr. OBERMAN. Thank you. Let me try to take all four of those in turn if I could.

Firstly, with respect to watch list effectiveness, what I can tell you is that today numerous U.S. government agencies are identifying known or suspected terrorist threats in and around the transportation system who would mean to do us harm. And that is happening in aviation and at border crossings and so forth, and it is of great concern to us, but of course we are very gratified that our systems are working to deter these people. And of course our capabilities under Secure Flight will be significantly improved. Of course, we need to be fully funded, I need to stress that again, so

that we are able to stand up the system and be as effective as we need to be to secure domestic aviation in the United States.

Secondly, with respect to privacy, let me reiterate that privacy is one of two goalposts for Secure Flight, the other of course being security. And that is a critical priority for us. This program is going to be as broad as anything the Department does. It will screen 1.8 million people flying domestically every single day in the United States. We need to be fully open and transparent with the American people and have total credibility with the American people to be able to effectively operate a system that is that broad.

And so we did issue a series of documents in September, and we made some adjustments to those documents a week ago today, as you point out, to more fully and clearly reflect exactly what we have been doing during our test period so that it would be on record exactly the nature of the test.

However, in addition to what is in the Federal Register, we have been up to brief congressional staff, committee staff. Numerous times we have given GAO literally hundreds of thousands of pages of documents and we have spent a lot of time with the media, the air carriers, the privacy groups and so forth so that, again, we have transparency and credibility with the American people. And the privacy documents, as I said, reflect that.

Finally, let me just say that with respect to the existing CAPPS I system that you alluded to, we do think it retains some security benefits. We do think it is, at least initially, more effectively operated by the air carriers, as I think Mr. May alluded to in his testimony, and our focus at the moment is standing up the system whereby we are going to check passengers against the watch list, as required by the statute.

Ms. JACKSON-LEE. And the professionalism training?

Mr. OBERMAN. I am not responsible for screener training at TSA—

Ms. JACKSON-LEE. I understand that.

Mr. OBERMAN. —but I will take it back, absolutely.

Ms. JACKSON-LEE. I have some further questions on the privacy issue, and I hope we will have an opportunity to provide you that in writing. Thank you.

Mr. LUNGREN. Time of the gentlelady has expired.

Let me just mention that the document prepared by the minority staff of the committee entitled, "Secure Flight's Missed Milestones," will be entered into the record in its entirety.

Now the gentleman from Massachusetts is recognized for 5 minutes.

Mr. MARKEY. Thank you, Mr. Chairman. I understand that ChoicePoint will not be involved in the Secure Flight Program; is that correct?

Mr. OBERMAN. Well, ChoicePoint is not involved in the test phase of the Secure Flight Program. We have not made any final decisions with respect to implementation. That will all be done in an open competitive process.

Mr. MARKEY. Well, I believe that ChoicePoint's contract would represent a poor choice for American taxpayers given the company's recent involvement in a massive privacy breach that has enabled hundreds of ID thefts, and I think you should know that is

how that decision would be viewed. The Pentagon recently confirmed that it had hired a Massachusetts company to protect personal information on potential recruits.

Beyond the Secure Flight Program, does TSA currently have any contracts with ChoicePoint or LexisNexis?

Mr. OBERMAN. I am not aware of any existing contracts with ChoicePoint. One of my contractors uses LexisNexis as a subcontractor but not for the provision of any data. We have some technology experts that help us with technology. We do not have any LexisNexis data.

Mr. MARKEY. Do you have any relationships with any companies that have been involved in privacy breaches?

Mr. OBERMAN. No.

Mr. MARKEY. None. None. Is TSA in negotiation with ChoicePoint or LexisNexis or any company that has been involved in a privacy breach beyond the Secure Flight Program?

Mr. OBERMAN. I am not aware of that, but it is obviously outside of my specific jurisdiction. I am not aware of any.

Mr. MARKEY. Has TSA always conducted security review of all contractors that access personally identifiable information, such as passenger name records before entering into contracts with third parties?

Mr. OBERMAN. Yes.

Mr. MARKEY. Has TSA ever terminated a contract with a third party contractor because it failed to provide adequate security to prevent unauthorized access to passengers' personal information?

Mr. OBERMAN. Not aware of that.

Mr. MARKEY. You are not. As you know, TSA recently admitted it collected personally identifiable information, such as passenger names, addresses and credit card numbers as part of testing for the Secure Flight Program. TSA's admission came after it reportedly stated it would not do so.

Given this retreat from its commitment to passenger privacy, why should this committee and the American flying public have any confidence that TSA will secure and safeguard passengers' private information when the Secure Flight Program is fully implemented?

Mr. OBERMAN. I respectfully disagree with the characterization that we retreated or changed what we have done. I want to just take a minute to explain that.

We developed a methodology for how this commercial data test would work in December, and from that point forward we have provided every document that we have generated and every document that our contractor has provided to GAO and in often cases directly to this committee and to other committees in the Congress. We have also fully discussed what that test would be with the media, the air carriers, privacy groups and so forth.

What we did in our most recent privacy notice was expand and clarify the discussion of commercial data testing that were in the documents that were issued in September. The September documents discuss our use of commercial data, and the June documents are designed to expand what was issued in September to reflect everything that was briefed between December and the current day.

And so there was no retreat or change. In fact, we are not making any changes to the manner in which the test is being conducted, because we do not need to. We just had to expand and clarify those existing documents, which is what we have done, and also I think it is important to note we have not taken any action against any passengers.

This was all using historical information from June of 2004 that we used our regulatory authority to collect and it is simply a test and it is being used to generate results, by the way, which are not yet conclusive, and so we decided to extend our test period so we can get better information.

Mr. MARKEY. I mean, I will just again for the record make it clear that privacy groups in America disagree with your assessment of the role that TSA is playing in protecting that information.

On May 20, I sent a letter to Secretary Chertoff along with Mr. Thompson and Ms. Sanchez regarding the Department's inability to check the names of international passengers against terror watch lists prior to departure of the flight to the United States. We have not yet received a letter in response to our letter.

Mr. Oberman, I believe our policy should actually be called, "no wheels up until the watch list has been checked off." What we have had as a policy is, "fly now and we will check the list later when the plane is in mid-air heading for the United States." When will the Department give us an answer to our question?

Mr. OBERMAN. I do not know, sir, but I will take that back and find out. That is the responsibility of Customs and Border Protection, and I will reach out to my colleagues today and find out.

Mr. MARKEY. So TSA has no role in that?

Mr. OBERMAN. That is correct.

Mr. MARKEY. Okay. So I would appreciate it if you could get us an answer. It is now a month and I think a month is a long time in homeland security terms to get an answer to such a question. We had two planes coming into Boston that both had to be diverted to Maine a month ago with people on board whose final security clearance actually had not been completed. And you just cannot have a system where potential terrorists are already on board and the final checks are now being completed back on land. It is just absolutely unacceptable, and TSA has a responsibility to get us this answer along with the entire Bush administration.

And, finally, could I ask him one final question? Any relation?

Mr. OBERMAN. To?

Mr. MARKEY. The famous Oberman?

Mr. OBERMAN. There are several famous Obermans.

Mr. MARKEY. Oh, there are?

Mr. OBERMAN. Which are you referring to?

Mr. MARKEY. That have television shows on MSNBC.

Mr. OBERMAN. Oh, it is spelled a little differently.

Mr. MARKEY. Oh, it is?

Mr. OBERMAN. Yes.

Mr. MARKEY. Oh, okay.

Mr. OBERMAN. He has got an L and a couple extra N's, I think.

Mr. MARKEY. Okay. Who was the famous Oberman that spells their name like you?

Mr. OBERMAN. My dad is a politician—

Mr. MARKEY. He is proud of you. He is very proud of you.

Mr. OBERMAN. He is more infamous than famous, but I was not sure if that is who you were referring to.

Mr. MARKEY. Okay. Thank you. Thank you.

Mr. LUNGREN. A Chicago politician.

Mr. OBERMAN. That is right.

Mr. LUNGREN. The gentleman from Oregon is recognized for 5 minutes.

Mr. DEFAZIO. Thank you, Mr. Chairman. I regret I was unable to hear the early questions. I was in the highway conference, which may or may not be coming to a conclusion soon.

If I could revisit the CAPPS I issues. When I was able to be here, one person testified CAPPS I had continuing value, another witness said it does not since it has all been on the front page of the USA Today. We know exactly what the criteria are, these terrorists are not casual people or people who may—they spent a lot of time planning the original attacks. It is likely they would have read USA Today, they visit Web sites, they would know what the criteria are.

Do you think that CAPPS I has continuing value, and if so, why?

Mr. OBERMAN. I do think it has continuing value, and the reason is that all of the criteria are not publicly known. So there are criteria that are still in use today that we think do provide a security benefit to identify passengers for further scrutiny, and we have made adjustments to the system directed at some of the criteria that are more publicly known that have dropped the selectee rates for CAPPS I significantly over the last 3 to 6 months.

Mr. DEFAZIO. So why wouldn't we just drop all the ones that are publicly known then, because some of those are ones that trip up business travelers. For instance, you know, you bought a ticket within 24 hours. Okay, well, what business traveler has not done that how many times this year?

Mr. OBERMAN. I would like to answer that question in a classified setting because it does not lend itself to a very simple yes or no answer with respect to how we would do that.

Mr. LUNGREN. If the gentleman would yield, while he was gone we talked about having a classified briefing on a number of elements that they are changing.

Mr. DEFAZIO. Great. Okay. Well, I would look forward to an explanation of that.

Let me ask this: We had another witness question the validity of the Trusted Traveler, as it is currently envisioned, and what the real benefits would be. Is a potential benefit of Trusted Traveler that if one were targeted under one of these CAPPS I criteria as a trusted traveler, a previous witness from TSA said you would look at the potential for waiving certain requirements of people, whether it is shoes or overcoats or laptops. Would it also be considered if someone was SSS by CAPPS I but they also had the Trusted Traveler card? Which one would trump?

Mr. OBERMAN. Today, participants for Registered Traveler are exempted from selectee screening if they are selected by CAPPS I. That is already in place today.

Mr. DEFAZIO. Okay. So you would envision that would—you have not had a problem or concern about that?

Mr. OBERMAN. No.

Mr. DEFAZIO. Okay. Well, I think the rest of my questions are really going to lend themselves to the classified portion.

When are we going to do that, Mr. Chairman, sometime soon, after the break or something?

Mr. LUNGREN. Well, we will do it as soon as we can schedule it.

Mr. DEFAZIO. Okay. Great.

Thank you, Mr. Chairman.

Mr. LUNGREN. Just a couple questions, Mr. Oberman. I would like us to be more explicit on the record as to the need for commercial database queries. As I understand what you were saying, when you have the watch list, if we have the full name and the birth date, that will take us down 60 percent of those who would otherwise be checked against the watch list. Then, as you say, your personal identifiers drop off rather significantly.

So as I understand it, that is when in addition to other sorts of classified data you might have, you would then utilize certain commercial databases as a way for determining whether the person who is standing there at the airport is in fact a person of real interest on the terrorist group; is that correct?

Mr. OBERMAN. Yes.

Mr. LUNGREN. And you are still in the testing phase of that?

Mr. OBERMAN. That is correct. In fact, we have just recently extended the test period, because we do not have conclusive results. They are very promising but they are not conclusive enough for us to be able to say this is exactly the way we would like to proceed, here is what it would cost and so forth. We are still testing.

Mr. LUNGREN. As I understand it, you would propose if you really rolled out the program that you would not own or retain the information from the commercial databases but rather you would be involved in a contractual situation where you would query these to find out positives or negatives in terms of the responses that you would wish to get.

Mr. OBERMAN. That is correct, and we would go one step further than that, which is we would destroy and discard all that information after the trip is completed. Do not need to retain any of it in our system at all.

Mr. LUNGREN. What about information that in fact cleared this person, tells you this person should not be on the watch list? You would get rid of the information that was utilized to do that but somehow you would identify that person thereafter as not being on the watch list?

Mr. OBERMAN. Yes. The way the system is structured is we are going to retain the so-called vetting history, which says that Ms. Smith was cleared. What I do not want to retain is any commercial available data because I am not going to use it for any further purpose. By virtue of having that vetting history, when the same Smith comes through the next day, I will know that that person was already in fact cleared. Assuming they have not been added to the watch list, they will be cleared again to fly, and they should not continue to be hassled.

In addition to that, some people will obviously go through the redress process in which they submit identifying documents to TSA, we place them on a cleared list, and we will be able to administer

that cleared list much more effectively than the carriers do today because we will be the only entity running the cleared list, and it will not matter to us what air carrier you are on. So those two features of the system will provide significant further reductions in the number of people stopped at the airport.

Mr. LUNGREN. So you are reducing that haystack we keep talking about.

Mr. OBERMAN. By a great deal.

Mr. LUNGREN. I thank you very much. I thank you for your testimony.

Mr. DEFAZIO. Could I have one—

Mr. LUNGREN. Yes.

Mr. DEFAZIO. Thank you, Mr. Chairman.

Earlier, the issue of the overseas travelers was brought up and the potential problems with the diversion of flights and that. And there were concerns raised about the logistical problems with early check-in or late check-in or whatever. I mean, to come to the United States of America or leave the United States of America or any other country, as far as I know, you have got to have a passport when you show up at the airport, right? And the ticket agent is going to look at your passport and then let you have the ticket. So they are going to see your passport, they are going to see the number, they are going to then transmit, I guess, that data to us at the airport.

Why couldn't we simply negotiate or try and negotiate with other countries that people when they make?this would get you down to a very small universe, which is people who fly internationally who book their ticket less than an hour in advance. If you said when you book your ticket you are going to have to give your passport information and then it will be provided to us as much as 6 months in advance, a month in advance, whatever, however long in advance that person made the reservation. Why wouldn't that work?

Mr. OBERMAN. Short answer is, I do not know why it would not work. It very well could. We are not responsible at TSA for vetting international flights which have unique attributes. All I would tell you is that I think that is something that Customs and the carriers are working on. I cannot—

Mr. DEFAZIO. Right.

Mr. OBERMAN. —speak to it beyond that, but of course that is the approach and maybe it is easier, although I do not feel like I have an easy job right now. That is of course the approach we are using for Secure Flight domestically, which is you will provide your full name and date of birth at the time you book your ticket. We are not going to look at your reservation until 3 days before because the watch list can change so much. And then between 72 hours and an hour or something before departure, that data will stream into TSA, be vetted, will provide results to the air carriers, notify the Bureau if there is a hit and start it again the next day.

Mr. DEFAZIO. Right. Well, I was involved in some of the discussions with the Europeans on the current system from the Aviation Committee during the last session of Congress. They had these huge privacy concerns about the data fields we wanted.

Mr. OBERMAN. Yes.

Mr. DEFAZIO. But there was never, as far as I know, any denial on their part that if that person is going to leave, say, Belgium or France and fly to the United States they have to have a passport to get on the plane. So I do not think that would go to their privacy concerns. I do not remember that it was raised at the time, because we had a whole other field of things that we were arguing over in terms of what disclosure would have to be made at the time of booking a ticket or at the time of embarkation in Europe.

But this seems to me fairly simple. I mean, if it is a document you have to have to get on the plane, then you have probably got it when you book your ticket, and if that information is provided then, we would get down to this really infinitesimal universe of people who are going to come here, buy an international ticket at the counter an hour before the plane leaves and that raises other questions about who that person is.

Mr. OBERMAN. I will be happy to take that back to Customs. That is easily done.

Mr. DEFAZIO. Okay. Thank you.

Thank you, Mr. Chairman.

Mr. LUNGREN. I thank you.

I thank you, Mr. Oberman, for your testimony, as I thank all the witnesses in the previous panel.

The members of the committee may have some additional questions for you, and we will ask if you would respond to them in writing. The hearing record will be held open for 10 days.

And without objection, the committee stands adjourned.

[Whereupon, at 12:32 p.m., the subcommittee was adjourned.]

○