AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TRANSPORTATION SECURITY ADMINISTRATION'S OFFICE OF INTELLIGENCE: PROGRESS AND CHALLENGES

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 14, 2006

Serial No. 109-83

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

32-739 WASHINGTON : 2007

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

PETER T. KING, New York, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

ROB SIMMONS, Connecticut, *Chairman*

CURT WELDON, Pennsylvania
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
STEVAN PEARCE, New Mexico
BOBBY JINDAL, Louisiana
CHARLIE DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
PETER T. KING, NEW YORK *(Ex Officio)*

ZOE LOFGREN, California
LORETTA SANCHEZ, California
JANE HARMAN, California
NITA M. LOWEY, New York
SHEILA JACKSON-LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

The Honorable Rob Simmons, a Representative in Congress For the State of Connecticut, and Chairman, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment 1
The Honorable Zoe Lofgren, a Representative in Congress For the State of California and Ranking Member, Subcommittee on Intelligence, Informaton Sharing, and Terrorism Risk Assessment 2
The Honorable Jim Gibbons, a Representative in Congress For the State of Nevada 16
The Honorable James R. Langevin, a Representative in Congress For the State of Rhode Island 14
The Honorable Nita M. Lowey, a Representative in Congress For the State of New York 12
The Honorable Stevan Pearce, a Representative in Congress For the State of New Mexico 18

WITNESSES

William Gaches, Assistant Administrator for Intelligence, Transportation Security Administration, U.S. Department of Homeland Security:
Oral Statement 4
Prepared Statement 6
Cathleen A. Berrick, Director, Homeland Security and Justice, U.S.Government Accountability Office:
Oral Statement 30
Prepared Statement 32

TRANSPORTATION SECURITY ADMINISTRATION'S OFFICE OF INTELLIGENCE: PROGRESS AND CHALLENGES

Wednesday, June 14, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT,
Washington, DC.

The subcommittee met, pursuant to call, at 2:40 p.m., in Room 311, Cannon House Office Building, Hon. Rob Simmons [chairman of the subcommittee] presiding.

Present: Representatives Simmons, Gibbons, Pearce, Lofgren, Lowey and Langevin.

Mr. SIMMONS. The quorum being present, the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment will come to order. Today the subcommittee meets to hear testimony on the Transportation Security Administration's Office of Intelligence and its integration within the DHS intelligence enterprise.

We will be hearing testimony from two witnesses today. Our first panel, we will be hearing from Mr. William B. Gaches, TSA's Assistant Administrator for Intelligence. Welcome, Bill. Good to have you here.

And our second panel, we will hear from Ms. Cathleen Berrick, Director of Homeland Security and Justice, U.S. Government Accountability Office.

I thank Mr. Gaches for being here this morning, and I also want to thank you for hosting our visit to your facility on Monday. The tour provided the subcommittee with insight for a look at how your office carries out its mission to identify, deter, and mitigate threats against our Nation's transportation infrastructure. And I look forward to continuing the discussion that we began on your role in protecting our Nation.

I also look forward to hearing from you today on the roles and responsibilities of the TSA Office of Intelligence and its role in the DHS intelligence enterprise. TSA's Office of Intelligence was created to mitigate the risk of terrorism against aviation. Formed in the wake of the 1988 Pan Am Flight 103 bombing over Lockerbie, the legacy Federal Aviation Administration's Office of Civil Aviation Security Intelligence was eventually transformed into a 24/7 operation during the Gulf War. However, the fate of the FAA's Intelligence Office was tragically changed on September 11, 2001.

Given these events, I found it very interesting and encouraging that one of the mantras of personnel from TSA's Office of Intelligence is, and I quote, zero tolerance for failure; no successful attacks against U.S. transportation based on failure by TSA intelligence to warn or inform.

The culture of TSA intelligence is emblematic of DHS itself. It is a culture of men and women that readily accept the responsibility to protect our Nation against the threat of terrorism. When I visited the office on Monday, I met a gentleman who worked for you, and I asked him why he chose TSA instead of the more traditional intelligence agencies like CIA or FBI, and he told me, and I quote, because here I am defending the homeland, unquote.

The good men and women that work in intelligence at TSA work hard every day to defend us against attack. That work is important. We must ensure as a Congress and as a government that they have the tools and policies in place to get the job done.

I would now like to recognize the Ranking Member of the subcommittee Ms. Lofgren for any statement she may have.

Ms. LOFGREN. I am pleased we are turning our attention today to the Transportation Security Administration's Office of Intelligence. The Department's Chief Intelligence Officer Charlie Allen recently testified before us about one of his key goals making all the Departments' intelligence offices work together. Put simply, Mr. Allen wants intelligence folks and TCB and to be on the same sheet of music when it comes to the intelligence agenda. To get there he needs the various intelligence offices falling under his leadership to share information with each other and to draw on each other's expertise in order to produce unique intelligence products, products that advise the Department's State, local, tribal, and private sector partners about what steps to take to protect people and property from terrorist attacks.

I therefore welcome the testimony here today and look forward to Mr. Gaches' testimony about the work he is doing. I look forward to asking both witnesses about the practical impact that TSA's intelligence shop has on everyday Americans. Specifically, I am interested with TSA's ongoing involvement and its impact on TSA's Secure Flight program.

Most Americans are well aware of news stories about senior citizens, babies, nuns and even Members of Congress being stopped at airports because they share the same or similar name as a terrorist on a watch list. In fact, a member of my own family is routinely stopped by certain airlines whenever he flies. I understand that TSA intelligence analysts are stationed at the Terrorist Screening Center at this very moment and are assisting in the monumental task of manually reviewing the tens of thousands of names included on the watch list based upon information we have recently received from the Department of Justice's inspector general. However, this manual review process will take 5 or 6 years to complete. We simply don't have 5 or 6 years to read through records to get the data right.

A similar data problem apparently plagues TSA's planned Secure Flight program. Ms. Berrick testified this past February the program, as presently envisioned, will rely upon the Terrorist Screening Center's terrorist watch list to conduct automatic name checks

to see if a passenger with an airline reservation is a terrorist or not. If the records on the watch list are inaccurate or incomplete, TSA's intelligence analysts along with their colleagues at the Terrorist Screening Center will have to perform a manual review of passenger records on sometimes very short time frames in order to see if they can figure out who is who. The same manual review will be needed if the airlines that submit passenger information to secure flights somehow muck up the data during the reservations process. Not only will this lead to delays, but I fear it won't protect us. Terrorists could game the Secure Flight system and also the current watch system.

As Ms. Berrick states in her prepared testimony today, Secure Flight was not designed to protect people using stolen identities from boarding airplanes. Given the millions of veterans' records recently stolen from the Department of Veterans Affairs complete with names, dates of birth and Social Security numbers, this vulnerability is a particularly serious one. Now that TSA has announced that its going back to the drawing board on Secure Flight, it might make sense to figure out how to address the identity theft problem as well as the inadequacy of name checks before getting too far ahead of itself. I therefore look forward to Mr. Gaches' comments not only about the work he is doing to stand up TSA's Office of Intelligence, but also how he is gearing it up to prepare for Secure Flight and to address the problems that Ms. Berrick and others at GAO have identified.

Welcome to you both, and I yield back, Mr. Chairman. Thank you.

Mr. SIMMONS. Thank you very much. And as the other members of the subcommittee know, they have an opportunity to insert any opening statement for the record that they may wish to insert.

Mr. SIMMONS. And it is a pleasure to have the distinguished gentlewoman from New York here with us this afternoon.

Our first witness will be William Gaches, who is the Assistant Administrator for Intelligence, Director of Intelligence and Analysis, Transportation Security Administration. He assumed this responsibility in February of 2006 and is the senior intelligence officer for the Transportation Security Administration.

From the year 2003 to 2004, Mr. Gaches headed the DCI's Terrorist Threat Integration Center, Analysis and Production Department, and was responsible for managing and overseeing all of TTIC's publication and analysis efforts. He is a 30-year veteran of the National Security Agency, has earned his BA in political science from Westminster College, received a master of liberal arts from Johns Hopkins University, and advanced certificate in American public policy from the University of Maryland in Baltimore. It is good to have you here.

We will put a 5 minute light on. We have your full testimony, so you don't have to read it. And if you wish to summarize in 5 minutes, we look forward to hearing your testimony.

STATEMENT OF WILLIAM GACHES, ASSISTANT ADMINISTRATOR FOR INTELLIGENCE, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. GACHES. Thank you, Mr. Chairman, Ranking Member Lofgren, for the kind opening comments. Members of the subcommittee, thank you for this time. It is an opportunity to talk to you about the Office of Intelligence at the Transportation Security Administration, our mission, our capabilities and some thoughts about how we use intelligence to help secure the transportation networks of America.

As I have not appeared as a witness before this subcommittee prior to today, allow me to a little bit more formally introduce myself. As Chairman Simmons said, I arrived at TSA in February of 2006. For over 31 years I served at home and abroad as an officer of the National Security Agency, including being the NSA production manager for counterterrorism from 2000 to 2003.

In 2003, as Chairman Simmons pointed out, I was indeed asked to be one of the founding leaders of the President's Terrorism Threat Integration Center, or TTIC, which later became the National Counterterrorism Center, or NCTC, and in this 2003 to 2006 timeframe, I did, in fact, run the analytic element of those organizations.

Along the way I became committed to the concept of team play, and also I became a colleague and, I dare say, a friend of Charlie Allen, DHS's Chief Intelligence Officer. As I headed, I thought, from NCTC back to NSA, Charlie Allen asked me if I would be interested in helping TSA improve their intelligence department. For me, a guy who wished to be a pilot in younger years and a college-age summer hire of a national airline, this would be too good an opportunity to pass up, action-oriented intelligence work coupled with transportation.

Administrator Hawley and I met, and by early February I was an assignee at TSA headquarters, but my commitment to TSA has steadily grown since that time, and on Friday, 12 May, I resigned from NSA and the following Monday came back to work as a TSA officer.

The mission of the TSA Office of Intelligence is, in fact, formally outlined in the Aviation and Transportation Security Act of 2001 and, in short, directs TSA to receive, assess and distribute intelligence information related to transportation security. This dynamic, multifaceted effort by TSA must be done in concert with the efforts of the DHS's Chief Intelligence Officer, his staff and DHS's other component intel shops. We cannot operate so independent as to preclude coordination and consultation with and across DHS, and we are, in fact, fully committed to the Secretary's objective as stated before the full committee this past October by Charlie Allen regarding integrating the intelligence elements of the Department, creating a unified intelligence culture, and improving the flow and reporting of intelligence.

This architecture building is, in my humble opinion, comparable to DOD's joint staff model. We are in the JCS/J2, work hand in glove with the J2s of the combatant commanders in the field, and each field commander's intel chief has their autonomy and their re-

sponsibilities, but one of those responsibilities is to work in concert with the JCS/J2 back in the Pentagon.

The intelligence office at TSA is comprised of 99 government personnel and about 40 contractors. We operate on a budget of about $21 million, most of which is used to pay for salaries, IT support and the critical IT linkage to the field and our customers. Organizationally we have three major components: a 24-by-7 watch operation at TSA headquarters, as well as intelligence officers at TSA's operation center in Herndon, Virginia; an analytic effort, which I view as our core purpose; and a business management team to help us run right and run straight.

Many of my analysts have prior intelligence and/or law enforcement backgrounds either in the military or at agencies such as FBI, DIA and CIA. Our products are transportation focused, and we strive to issue much at the lowest classification level possible, frequently to include unclassified reports.

We have two primary customer sets. First, the major transportation industries, aviation, mass transit and rail, maritime, cargo, highway, and pipeline; and our second primary customer is the operational element of TSA, almost the rest of TSA, which includes 150 TSA Federal security directors and 40,000 transportation security officers, formerly known as screeners, supporting 450 federalized airports and associated intermodal transportation activities across the country, as well as 21 Federal air marshal field offices. Working together, we help to operationalize the intel and put it to work to secure our transportation networks.

We also interface daily with and draw upon the U.S. Intelligence Community as well as other U.S. Government agencies. We consider all forms of intelligence as critical to our mission, and we also rely heavily on open-source information to include information garnered by the transportation industry, and by TSA officers in the field at passenger checkpoints, and by TSA's Federal Air Marshal Service.

We are not, nor should we be, construed as experts in all things terrorism, but we need to know where to go to get that expertise, then operationalize this intelligence and make it work for our customers. The intelligence analysts at TSA needs to comprehend facets of transportation and simultaneously the implications of the intelligence covering terrorists' intentions, plans and activities.

In conclusion, the future for the Office of Intelligence will be challenging, as is any Office of Intelligence engaged in the global war on terrorism. Our adversary is determined, learns from its mistakes and is flexible in many ways. We will focus on training our workforce and on continuing to work with DHS, the U.S. Intelligence Community, and our customers. This is a battle that cannot be won by one agency or even two or three. It will take a collaborative and cooperative approach across DHS and across the U.S. Government. As the Assistant Administrator For Intelligence at TSA, you have my pledge that I will do all that I can within authorities in law to ensure the safety of the United States' transportation networks.

Thank you for this opportunity, and I welcome your questions.

Mr. SIMMONS. I thank you for that testimony.

[The statement of Mr. Gaches follows:]

PREPARED STATEMENT OF WILLIAM GACHES

Good morning, Chairman Simmons, Ranking Member Lofgren, and members of the Subcommittee. Thank you for this opportunity to speak with you about the Transportation Security Administration's Office of Intelligence (OI) and its crucial role in assuring transportation security. OI serves the Assistant Secretary, key TSA staff, TSA field elements and a select, specialized set of stakeholders located mainly in the transportation sector. As such, its efforts complement and are coordinated with the broader mission of the Department of Homeland Security (DHS). Today, I would like to address who we are, what we do and our ongoing efforts to improve intelligence at TSA.

Our Mission

The layered approach to security seeks to identify and deter threats well before they reach America's airports, railways, highways, mass transit, and ports and pipelines. United States government agencies work with others around the globe to identify and disrupt terrorist activities at their source. U.S. Customs and Border Protection activities further identify potential terrorists and bar their entry into the United States. Federal, State, and local law enforcement work together with the FBI in Joint Terrorism Task Forces across the United States to identify and disrupt terrorist activities within the country. Intelligence activities are vital to the success of this effort and TSA's OI is a key part of the intelligence team.

Although many of TSA's most visible programs, like aviation checkpoint screening, are intended to deter and physically prevent terrorists from carrying out a planned attack, the reality is that much of what TSA does is focused on stopping terrorists before they launch an attack. OI is absolutely critical to that effort because information, analyzed and shared, is the very heart of this defense. That is why we are working to enhance TSA's role as an information resource to support our partners and stakeholders in transportation security. Our goal is to make sure that our government and private sector partners receive timely information from us and communicate directly with us so we can achieve maximum effectiveness in our response to terrorism and ideally in its prevention.

OI is legislatively mandated by the Aviation and Transportation Security Act of 2001 (ATSA), further revised by the Homeland Security Act of 2002. ATSA directs TSA to receive, assess, and distribute intelligence information related to transportation security; assess threats to transportation; develop policies, strategies, and plans for dealing with threats to transportation security; [and] act as the primary liaison for transportation security to the intelligence and law enforcement communities. . .″

OI is the intelligence organization for TSA, providing an organic capability to review, synthesize, and analyze transportation specific intelligence. It is the only federal intelligence entity focused solely on security of the transportation sector. OI coordinates closely and shares information with other DHS components, the intelligence and the law enforcement community, other government departments and agencies such as DOT and FAA, and the transportation industry. To facilitate collaboration with the intelligence community and provide rapid analysis and notification of threats, this office has placed liaison officers with key intelligence community and law enforcement agencies across the Federal government.

OI is critical to TSA's overall risk-based security strategy. Its products provide a threat framework to prioritize security resources which is regularly used by the Federal Air Marshal Service, Federal Security Directors and the transportation industry. The office operates and maintains a twenty-four hour a day, seven days a week intelligence capability for TSA and, in conjunction with the Transportation Security Operations Center (TSOC), disseminates warnings and notifications of credible and imminent threats.

In order to perform its mission, OI provides and maintains the information technology (IT) infrastructure for interfacing OI with U.S. Government classified networks. It also maintains secure electronic connectivity to over 190 TSA field elements via the Remote Access Security Program (RASP) that provides the TSA field with access to classified information in a timely and secure manner.

It must be stated that TSA's OI is one part of the team at a complex and multifunctional Department of Homeland Security. We are fully committed to the Secretary's objective as stated before the full committee this past October by Charlie Allen, DHS's Chief Intelligence Officer, of integrating the intelligence elements of the Department so as to create a unified intelligence culture, improving the flow of intelligence information both horizontally and vertically throughout the organization, and improving the reporting of intelligence information from the Department's operating components and providing actionable, relevant analysis back to them.

The Office of Intelligence consists of two Divisions. The Intelligence Watch and Outreach Division functions as a 24/7 watch, providing indications and warning information related to transportation security while fulfilling vital communication and liaison roles. The Current Intelligence and Assessments Division assesses current and emerging threats across all modes of transportation and creates products that are key to shaping security policy and developing and implementing countermeasures.

Intelligence Watch and Outreach

Our Intelligence Watch and Outreach (IW&O) Division employs a cadre of experienced intelligence officers who operate and maintain a 24/7 intelligence watch capability for TSA. The essential goal of their efforts is to identify and assess the credibility of any security threat(s) to U.S. transportation, to alert OI and TSA managers and staff to these threats, and to support OI, TSA, and other U.S. Government organizations in their efforts to deter and prevent credible planned or actual attacks against U.S. transportation by providing Intelligence indications and warning support and crisis management assistance.

To support this mission, IW&O maintains a full-time liaison officer presence at seven key Intelligence Community (IC) and Law Enforcement (LE) nodes including DHS's Office of Intelligence and Analysis, the Director of National Intelligence's (DNI) National Counter Terrorism Center, the FBI's National Joint Terrorism Task Force, Customs and Border Protection's National Targeting Center, the National Security Agency (NSA), the DEA-administered El Paso Intelligence Center (EPIC) Air Watch, and the Terrorist Screening Center (TSC). These liaison relationships facilitate the timely analysis and exchange of intelligence relating to transportation security and also provide these other entities with valuable expertise in transportation security as well as real time access to our experts and capabilities in the OI.

In addition to the Headquarters Watch operation, IW&O also maintains an OI office (24/7) at TSA's TSOC. In that capacity, it provides direct intelligence support to the TSOC and the Federal Air Marshal Service's Mission Operations Center. The office also develops and executes all OI field support and Intelligence Operations outreach programs.

Current Intelligence and Assessments

OI's Current Intelligence and Assessments (CI&A) section is a well experienced group of intelligence officers whose products and programs focus on the terrorist threat to transportation. These professionals perform valuable functions in support of daily security readiness and long term strategic planning. Among their products are:* The Transportation Intelligence Gazette (TIG), Weekly Field Intelligence Summary (WFIS), Suspicious Incidents Report (SIR);* Specialized analytic assessments focused on terrorist groups, weapons, explosives, Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive threats (CBRNE), modus operandi, tactics and trends;* Baseline modal threat assessments, updated as developing information warrants; and* Special reports and other products as needed to support the intelligence needs of TSA, DHS, and the intelligence and law enforcement community.

Significantly, CI&A provides intelligence support for other TSA Assistant Administrators, notably Transportation Sector Network Management (TSNM) and its modal general managers, Security Operations, and Law Enforcement/Federal Air Marshal Service. CI&A products assist these critical TSA components in assessing risk, to include consequence, criticality and vulnerability, and developing appropriate security programs, countermeasures, mitigation strategies and protection guidance.

CI&A's focused examination of data to identify new or unrealized threats in the transportation domain assists TSA leadership in understanding the strategic threat. Analytical products are used in the development of security policies and the setting of program priorities. Transportation intelligence assessments often serve as the key ingredient in shaping Security Directives (SDs) and Emergency Amendments (EAs) to stakeholders and support decisions on countermeasures. Frequently, CI&A coordinates on issues related to the National Infrastructure Protection Program (NIPP), National Strategy for Transportation Security (NSTS), National Planning Scenarios, Strategic Homeland Infrastructure Risk Assessment (SHIRA), Transportation Security Operational Plan (TSOP) and other similar programs. CI&A also plays a critical role in the development and coordination of interagency security initiatives. The Division's Director serves as TSA's technical advisor to the Overseas Security Advisory Council (OSAC) of the Department of State and directs TSA's Chemical and Biological Task Force, which, in turn, provided countermeasures support to the TSA Pandemic Influenza Task Force.

OI directs TSA's Red Cell activity to identify potential vulnerabilities in the transportation system through the use of adversarial (terrorist) role playing and scenario

development. All major offices of TSA participate in the Red Cells, to include TSA field personnel, Office of Security Operations, TSNM, OI, Internal Affairs, Information Technology, Operational Process and Technology, Office of Chief Counsel, and Office of Law Enforcement/Federal Air Marshal Service. Red Cell members reflect TSA's broad knowledge, expertise and ability to think creatively and outside-the-box. The purpose of the TSA Red Cell is to provide TSA leadership with threat scenarios that could affect the U.S. transportation infrastructure so that mitigation strategies are developed to counter these vulnerabilities. Following the presentation of the Red Cell scenarios to TSA senior leadership, other TSA offices conduct criticality and consequence analysis, determine appropriate counter measures and validate mitigation strategies. U.S. transportation sector representatives and industry stakeholders are made aware of these Red Cell scenarios which pinpoint potential vulnerabilities to the transportation system so that they may assist TSA in the development of mitigation strategies.

In support of transportation stakeholders, CI&A coordinates with Information Sharing Analysis Centers (ISACs) to ensure awareness of and maintain a baseline understanding of threats to all modes of transportation. The Department, working with the Federal Transit Administration (FTA), coordinates information and threat sharing for rail and transit through the Surface Transportation Information Sharing and Analysis Center (ST-ISAC) in partnership with the Association of American Railroads (AAR) and the American Public Transportation Association (APTA). As part of the significant partnership that has developed, TSA hosts ST-ISAC representatives at the TSOC. Similarly, CI&A, in coordination with security program officials at DHS, TSA, and DOT, shares threat information with highway, trucking, and motor carrier stakeholders through the Highway Watch program. The TSOC maintains a working area and supporting equipment for this program as well.

Across the critical infrastructure sectors, including transportation, DHS is streamlining governmental organizational structure and processes to improve coordination and engagement with industry stakeholders. Government Coordinating Councils (GCCs) have been established to implement the public-private partnership envisioned by the National Infrastructure Protection Plan. The Transportation Sector GCC formed in January 2006. That council is establishing its membership and operating procedures, direct formation of modal GCCs, and facilitating outreach to stakeholders to foster development of equivalent Sector Coordinating Councils (SCC) for each of the transportation modes and the sector as a whole. Membership includes TSA as Chair, DHS, Department of Transportation (DOT), Department of Defense (DOD), and the Department of Energy. GCCs in each of the modes are developing strategies, plans, and initiatives for transportation security.

The intelligence professionals at TSA OI provide essential all-source, all modal, foreign and domestic transportation threat intelligence analysis capability in the United States Government.

The Path Forward

The spectrum of its transportation security responsibilities, TSA seeks opportunities to enhance security posture and activities through targeted deployment of resources. In the intelligence field, OI has established a Pilot Program to enhance reporting of information obtained incidental to law enforcement and security operations, by deploying Field Intelligence Officers to a select group of airports including Boston, New York (JFK International Airport), Miami, Chicago (O'Hare International Airport), Los Angeles (Los Angeles International Airport), Phoenix and Dallas Fort Worth. Our goal is to improve intelligence support, coordination, and communication between TSA Headquarters, our Federal Security Directors (FSDs) and our modal stakeholders. After a one year trial, the Pilot Program will be evaluated.

The Field Intelligence Officers will serve as the principal advisor to FSDs and their staffs on all intelligence matters. Other responsibilities will include developing and maintaining a working relationship with local, federal, state, and private entities responsible for transportation security, regardless of mode. It is important to note here that while our officers will be based at the airports, they will still interface with the security elements from the local rail, mass transit, highway, and port and pipeline (where applicable) modals to facilitate the sharing and exchange of relevant threat information among these modals. TSA Field Intelligence Officers will gather pertinent law enforcement and intelligence information and ensure it is disseminated throughout the National Intelligence Community. Law enforcement information will be vetted, validated, and formatted as Homeland Intelligence Reports (HIRs) by TSA's Office of Intelligence HIR program. Upon approval, the HIRs will be disseminated to the Intelligence Community.

Field Intelligence Officer core competencies will include:* delivery of intelligence briefings to FSDs, senior staff, airport workforce and partner agencies;* service as

intelligence liaisons with applicable federal, state, and local intelligence offices;* the facilitation of intelligence data sharing from TSA Headquarters via the Office of Intelligence; and* submission of field intelligence reports to TSA Headquarters via the Office of Intelligence.

Staffing for the Field Intelligence Officers will rely on highly competent and experienced personnel. These officers are expected to interact and coordinate with multiple levels of government and non-government personnel at each site. The Field Intelligence Officers will serve as the face of TSA's Office of Intelligence for thousands of TSA employees working at the airports.

Operational support derives from the TSA Assistant Administrator for Operations and the FSDs at the seven participating airports. TSA's Office of Intelligence has sufficient staffing to support the Pilot Program.

Conclusion

TSA's Office of Intelligence serves a select, specialized community of TSA leadership and key stakeholders. Our position within the government draws upon the expertise of experienced intelligence officers whose focus on the transportation industry provides the intelligence and law enforcement communities with valuable resources with which to prevent a terrorist attack. By providing an organic capability to review, synthesize, and analyze transportation specific intelligence, we make an absolutely critical contribution to our nation's security which complements the efforts made in the Department as well the government as a whole.

Thank you again for this opportunity to inform the subcommittee of our efforts. I would be happy to respond to any questions that you might have.

Mr. SIMMONS. In my opening statement, I referred to the TSA's Office of Intelligence slogan, I guess you could say, zero tolerance for failure. You know, air traffic is one of those modes of transportation where somebody like myself who is inherently scared of flying wants to make sure that the takeoff, the flight, and the landing are done 100 percent perfectly. We don't want 95 ercent of the takeoffs, the flights, and the landings to be successful, you know. That 5 percent of lack of success is what scares us all when it comes to flying.

And certainly after 9/11, great efforts have been made by the U.S. Government and by TSA intelligence to improve the security of those flights. But in so doing, we also have to balance the privacy issues of the traveling public with efficiency issues, the efficiency of getting people through the security process and to their aircrafts in a timely fashion so that they don't—they don't miss the flight.

What do you see as the principal challenges of your office, of TSA intelligence, and in balancing that security with that efficiency'

Mr. GACHES. The challenges that I see in that particular case, Mr. Chairman, would be largely surrounding first and foremost, we are concerned about the privacy of the American citizen, and as the recipient of the no fly and selectee list from the Terrorist Screening Center and the responsible agent for forwarding that on to the U.S. airlines in which they do the actual matching with oncoming passengers, we work as hard, as Ms. Lofgren pointed out, and also in a very manually intense system right now to try and ensure the privacy balanced against what we know is out there trying to work through our system. And it becomes very difficult because, as I pointed out in my oral testimony, this is an ever-changing enemy; this is an enemy that is becoming increasingly difficult to identify. This is an enemy that was not quite what it was in September of 2001 or before that.

So this is a constant balancing act between where we are trying to preserve the rights and the privacy of American citizens while still being able to determine where the bad person is, if you will,

and how they are trying to get through whether it is the aviation or any other transportation system, a constant balancing act. A lot of training for our analysts to be witting of privacy concerns. It is done on an annual basis. So we are trying on many different facets to balance between both of those very important tasks for the office.

Mr. SIMMONS. And I am sure you have heard of the stories about the little baby whose name is Osama bin Laden, or, in my case, the treasurer of the Connecticut Education Association whose name is Michael Freeman, whose name matches the name of somebody else, and when they get slowed down in the process, then we have to try to correct those holdings for those individuals.

How efficient and how effective do you feel we have been in addressing those issues?

Mr. GACHES. I think we have made some progress. I think we have a long way to go yet, in all honesty. This is a very complicated process, in an open hearing and unclassified. I know that you all are familiar with the basic tenets of how this works, the information that we receive from the TSC, how that information is fed to the TSC in the first place. It is a process that when you just look at it almost in a flow-chart fashion has room, unfortunately, for error just because of the complexity and the volume and the variety of the input of the information.

I would certainly welcome you, Mr. Chairman, and Ranking Member Lofgren, to TSA for a classified sort of A-to-Z review of this process. There are things that I would be perhaps incorrect in a public forum to detail about some of the checks and balances that we can take, and certainly don't want to give those away in an open forum, but would be happy to have all of the members of this subcommittee visit us and have members from the TSC and from the National Counterterrorism Center and other parts of the community have a discussion about this entire process. I think you might find that very useful and helpful and also answer some of the questions that might be difficult to address in an open forum here.

Mr. SIMMONS. I appreciate that.

One final question. We all hear about the exceptions to the rule where the wrong person is identified or stopped or delayed. Am I correct in assuming that there have been instances where the right person or a person who is on a terrorist watch list has also been identified and either detained or otherwise questioned?

Mr. GACHES. Absolutely. A very recent and exciting adventure that we took part in, actually led a few weeks ago, where through other sources we had six individuals, five individuals identified on a particular flight, and, in fact, they were on that list that we call the no fly List. They were bona fide flyers. They had unfortunately gotten onto the flight because it was coming from an overseas location, so because we knew who they were, we could confirm that. They were greeted accordingly and followed accordingly by law enforcement agencies to determine what they were up to, et cetera. And, again, wouldn't want to go into any further detail, but I would say certainly several times a month we are getting positive hits on this system.

Mr. SIMMONS. Thank you. My time has expired, and I recognize the distinguished Ranking Member.

Ms. LOFGREN. Thank you, Mr. Chairman.

I am wondering, Mr. Gaches, the GAO recently concluded that TSA's response to the problems in Secure Flight raise more questions really than it answered. And I am wondering, they pointed particularly to the accuracy and completeness of the records included in the Terrorist Screening Center's master terrorist watch list in the database as well as the protocols for handling airline reservation information in a way that facilitates the TSA-based Secure Flight automated name-checking process; and then also the role of TSA OI analysts in ensuring that false positive, innocent people are identified and then dealt with effectively. Can you address those GAO criticisms here in a public session?

Mr. GACHES. Thank you for that question and the opportunity to make a left turn.

Let me say in all honesty, I am clearly not the Secure Flight expert, and, in fact, it is not a direct responsibility of the Office of Intelligence. It is a complicated process, as you are aware, because of the vast number of inputs and the variety of agencies that input to the TSC and eventually in the case right today of the no fly and selectee list.

Certainly the Secure Flight program first and foremost is being revamped and built from privacy up to standpoint, and our goal is to do it right and not do it fast. And as I think you are aware, we are rebaselining that program, and I am sure Cathy will have more words to say about that from the GAO perspective.

I think that in the entire—if I may say that in the entire war on terrorism, it is difficult to always have precise information on the individuals that you are looking for, and the details on precise information, that probably should be left out of this open hearing. And we would welcome you again to go through in a classified session what we use criteriawise, why we encounter problems, and some thoughts that we have, and perhaps solicit thoughts from you that we should employ in making this a better and faster system, because clearly we do have room for improvement.

Ms. LOFGREN. I am wondering, you mentioned in your testimony that you have information on a daily basis from the Intelligence Community. To what extent do you have connectivity with the Intelligence Community? What kind of interface do you have that permits the full sharing that we expect?

Mr. GACHES. Thank you for that.

As I mentioned, I have come out of that Intelligence Community. I have accrued a few friends and contacts that will still talk to me even in the non-IC status that I now hold.

As you know, the TSA Office of Intelligence is not one of the formal 16 members of the U.S. Intelligence Community. Formally, however, let me point out perhaps one of the most critical things, even though it sounds somewhat elementary.

Each morning the Administrator and I start our intel day by attending a televised secure videoconference with, I will just say, lots of folks talking about lots of things, and it is hosted by the National Counterterrorism Center, and Admiral Redd, Retired Admiral John Scott Redd, is the host of that. And in that forum we have

the opportunity to sort of have the huddle, have the scorecard check, if you will.

That doesn't stop at that time. There are other video teleconferences then the rest of the 24-hour day involving very many of the same organizations, usually different sets of players, if you will. That is one of the best ways to keep connected. We are an active participant in the Interagency Intelligence Agency on Terrorism. We are an active participant and supplier, if you will, of liaison officers, who—I will just say from various parts of the Intelligence Community, and, of course, there is the thing, this network, of just keeping in touch with those you used to work with.

Ms. LOFGREN. Well, could I ask just more in a systemic way—systematic way, I don't want to denigrate those informal, because I am sure those are very important, but I am interested, we have accumulated or supposed to have accumulated intelligence information, various databases, one of which is the customs enforcement arm, Immigration Customs Enforcement. To what extent do you have technology that can interface with ICE and utilize that database to inform the decisions on the terrorist watch list? And can you talk about specifically the computer systems and other software programs that you have?

Mr. GACHES. I apologize. I could not very well address the computer systems of the IT connectivity between specifically ICE and those databases that are used in the watch list process, or even to the Office of Intelligence. That is clearly an area that we need to grow our connectivity to CBP, to ICE, and the Coast Guard is an area that both my Deputy and I are very interested in trying to move forward and bring a closer connectivity between the component intel parts of DHS as well as to DHS's own IA central activity.

Ms. LOFGREN. I wonder if you could follow up subsequent to this hearing with the details on that question.

Mr. GACHES. Sure. I would be happy to do that.

Ms. LOFGREN. Thank you.

Mr. SIMMONS. Chair recognizes the gentlelady from New York.

Mrs. LOWEY. Thank you, Mr. Chairman.

And thank you very much for appearing before us, and I would like to pursue this line of questioning because in my district, there have been at least five different examples of constituents that have contacted my office about possibly being placed on a watch list, and in each case, it seems as though they are a false positive and don't deserve extra screening.

One case in particular, which I think we finally sorted out, this person was a Peace Corps worker in Africa 20 years ago, and he rides first class, he rides frequently. He has an international business. He lives in Westchester County. He must have names similar to others on the watch list, and each case he still has to arrive several hours before he boards the plane. And I hope the most recent effort that my office has made will take care of this.

But it seems to me that your intelligence office has or should have a central role in TSA's current redress process, and my understanding is that innocent travelers now supply additional information about themselves to TSA to distinguish themselves from those on the terrorist watch list.

And we want you to do your job because we understand that the safety and security of the public is at stake here; however, this particular case and a half dozen others that have been brought to my attention just seem to me to be a lack of efficiency, or that is what I am trying to find out. What is going on? Could you tell me the average amount of time it takes for an innocent traveler to clear his name?

Mr. GACHES. Thank you. No, I could not, because the Office of Redress is the one that has those statistics and runs that activity where an individual who wants to fill the paperwork out and the forms to have their name or similar name, if you will, removed and clarify them as not being the party of interest, they maintain that. It is an entirely separate operation from me. We occasionally get involved, depending on the particulars of the case at hand.

I am not familiar with the individual that you mention from Westchester. I would be happy to take additional information perhaps after this or through your staff and personally look into this on your behalf, but the general process is that the Office of Redress at TSA will take the information from an individual. They will return to us and to the TSC to compare that information with that which is held in the databases, and then we can go from there. We have gone to some—at some points issuing letters for individuals to carry to explain to the carriers. This takes—sometimes this will take, unfortunately, a lot of time to get the records cleared all the way back through the various carriers.

Mrs. LOWEY. But, Mr. Gaches, don't you have a voice in who makes the no fly list? Has the Terrorist Screening Center drawn the expertise of your office from making decisions?

Mr. GACHES. In this setting I would just say that the preponderance of the no fly and selectee individuals are nominated by other agencies, and TSA has a limited role in doing that because this comes from, we will say, core intelligence agencies and law enforcement agencies. We at TSA Office of Intelligence seldom—certainly not in the 4 months I have been there—have nominated individuals for either of these lists.

Mrs. LOWEY. Well, one of my concerns, not just with DHS, but I have seen this happen with many of the agencies of government, is the lack of coordination, and it seems to me that we have had three attempts at least to put in place an automated passenger screening system, and if you don't know the role and responsibilities of your people, how would the program be designed in ways so they are going to work together' Because it seems that the integration of these offices should have been addressed in the planning stages of the program.

Maybe you can explain how that works, and if someone is applying for redress, shouldn't the Intelligence Office be involved' Shouldn't an intelligence analyst look at what evidence there is and what questions should be asked, and who else has the background and knowledge at TSA to inform the discussion of who is and who is not a terrorist?

Mr. GACHES. I would again comment that our office's purpose is more in the liaison with the airlines' at the beginning. On a redress issue, we would have—we could help facilitate going back to the originator of that individual being placed on the list, and 99 per-

cent of the time, 99-plus percent of the time, that is not the TSA Office of Intelligence who nominated that person in the first place. So we would have to go back to the originating agency and ask them for further details, tell them the information that the Redress Office has.

And I take your point. We could perhaps be more proactive in facilitating that between the Office of Redress and whatever element of the Intelligence Community or law enforcement community nominated the name in the first place. But by and large, that is not a role that we have had a leading role in, if you will.

Mrs. LOWEY. My time is up, but let me just say, Mr. Chairman, if I may, I am concerned that we are not doing enough to examine these names, and if we ever reach a time where we need to focus our resources on an imminent threat, the terrorist list will be needlessly populated by people who pose no threat, and we will not have separated those individuals who should not be on the list from those who should; and that we are going to be overwhelmed by a list which is so long and unrefined that it defeats the very purpose of a list, which is to focus on the real threats.

So I am concerned that there are so many of these units that have particular responsibilities, and I wonder about the overall coordination and what your office is actually doing to refine these lists, but I guess we can take that up another time unless the Chairman—maybe you could pardon? Okay.

Mr. SIMMONS. We plan to have a second round of questions. I think the gentlelady's comments are well taken, and I think that, as I understand the process both from the witness and talking to others, the Office of Redress goes back to the originator of the information, and in these particular instances, if TSA intelligence is not the originator of the information, let us say it is FBI or CIA or somebody else, they would not be directly involved.

But I think what you are suggesting, which is quite correct, is that we have to facilitate and improve the process of cleaning up these lists, because if my constituent is on the list with several other people by his name, and one of those people is a dangerous person, we want to make sure that it is the dangerous person that is being apprehended and not everybody else. And, you know, that goes to the issue of trying to improve the process, and that is what oversight is all about.

And now I yield to my friend from Rhode Island, the distinguished gentleman Mr. Langevin, who has been very patient.

Mr. LANGEVIN. Thank you, Mr. Chairman.

And, Mr. Gaches, thank you for your testimony today. And I echo the sentiments and comments of many of my colleagues. We are concerned—we obviously want the potential terrorist watch list to be accurate, and the sooner we can make sure that that list is culled and that we have an adequate redress process, the better, because I don't think there is a member in Congress that hasn't had a constituent or someone they know directly that has been on that list and shouldn't be because they were looking for a list—the list itself was looking for someone else.

Turning to another front, though, we have heard from Chief Intelligence Officer Charlie Allen about his plans for a new Office of Intelligence and Analysis, and his plans to integrate the various in-

telligence components as a united intelligence operation. So it seems to me that IA must decide if it is going to be either a strategic-type operation that focuses on setting an agenda, policies, and representing intelligence components like your shop to the wider Intelligence Community, or an operational shop that is going to be creating its own intelligence products.

So my question is what path is IA taking, in your view, and what path should it be taking, and how is IA's approach working for your shop?

And my other question would be how does TSA's Office of Intelligence work to ensure that your analyst expertise informs what IA is producing, and what challenges have you encountered in this area?

Mr. GACHES. Thank you, sir, for those questions. On the first—I think that the DHS IA approach to being the strategic sort of ombudsman for the Department in having cognizance of and looking at the strategic assessing of issues related to the component intel parts is the way to go. DHS IA has to cover everything in regards to the homeland. I am somewhat of a specialist. I am the transportation systems or networks intel officer. I am not saying that I don't care about other aspects of the terrorism problem, but that is where my focus really has to be, and I am much more tactical than the DHS IA activity in the sense that I am on the phone or my folks are on the phone with someone at Amtrak, someone at a particular airline, whatever the case may be. DHSIA, I see them, and I am hoping, and I think from conversations with—Charlie Allen sees them more of a strategic view.

Now, we are just beginning, as I mentioned in my opening comments. This is an architecture that is a work in progress, and we have got some load-smoothing to do and some bumps to iron out, but that would be my response to the first part of your question.

As far as how we sort of work, I think your second question, more almost on a day-to-day, how do we fit into IA as far as ensuring analytic conversations and collaboration, we are in no small part in constant contact both visibly and physically, if you will, with the individuals at Nebraska Avenue. Each of my modal transportation analysts have an individual or individuals IA that they have the ability to reach out to. We try and inform and in many cases coordinate on the work that we do. They are the recipients—they, being IA, are the recipients of everything that the Office of Intelligence at TSA produces. So I think, you know, we are providing them everything that we are doing. We certainly have access to all that they produce, but I would just ask you to consider keeping in mind that we are servicing that very focused area—not small, not insignificant by any stretch of the imagination, but we are transportation focused, and DHS IA has to look across the gamut of things that are homeland security issues.

So we are actually complementing each other, and as I said again in my opening comments, not too dissimilar from the JCS/J2 model where if you are the J2 at the Pentagon, and you want to know something about what is going on in Bolivia, as an example, chances are you are going to reach out to the J2 at SOUTHCOM who really has some expertise and is focussing in on

there, and then that relationship exists between those two, just like it does between Charlie Allen's folks and myself.

Mr. LANGEVIN. Within the Department, do you believe that you have timely access to the accumulated DHS intelligence base' That is, can you easily retrieve—I mean, manipulate information or intelligence that, for example, Immigration and Customs Enforcement, for example, has collected; and if so, by what means do you access this information' Specifically which systems do you use?

Mr. GACHES. Thank you.

In all honesty, I don't know the names of the systems, if you will. But we do have the ability to reach out and electronically obtain the Customs and Border Patrol reports, the ICE reports, the Coast Guard reports, all of the DHS components, as well as the Intelligence Community component reporting.

Now, there are limitations. I can't say that we have access to 100 percent of everything that is out there. And in some respects we probably don't even need access to 100 percent of everything out there because of our niche approach, if you will, to a lot of the issues. But I feel comfortable that my analysts are able to go through both the classified and the open source through our IT connectivity, which is very robust, with all of component intel parts of DHS, as well as with the Intelligence Community members themselves, and I feel fairly comfortable in the way and the speed with which we can do that. And that is in addition to conferences and meetings and just telephone conversations, and very often like-minded analysts or subject matter experts gravitate together and exchange information as well.

That is sort of the informal network. So I think we have it fairly well covered for both informal as well as electronic connectivity.

Mr. LANGEVIN. I thank you.

I see my time has expired, but, again, thank you for the answers to my questions, and we certainly look forward to working with you to make sure that this effort is as robust as possible to make sure the work that you are doing is maximized. Thank you.

Mr. GACHES. Thank you.

Mr. SIMMONS. I thank the gentleman for his questions.

The chair now recognizes the gentleman from Nevada.

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

Mr. Gaches, thank you very much for being here today and for your testimony.

Basically what distinguishes or differentiates TSA's intelligence from Homeland Security intelligence?

Mr. GACHES. Thank you, sir. If I may, I am assuming you mean specifically how do we differ from intelligence and analysis——

Mr. GIBBONS. Analytical.

Mr. GACHES.—IA, if you will, at DHS headquarters.

I would offer that we are very focused on transportation. That is our niche. That is our lane, if you want to call it, in the road. IA is very much looking across the board of all sorts of issues related to homeland security that may or may not have a transportation and terrorism nexus. I think we are also much more tactical in many respects.

One of my goals and one of the Office of Intelligence's goals is this doesn't do us any good, this intelligence, if we can't get it out

to somebody who can use it and make a difference, whether that is in the industry, or whether that is an operating element of TSA, such as the Transportation Security officers at the airports, the Federal security directors located across the country, the Federal air marshals. Any of those thousands of people are our customers as well as the transportation industry folks themselves. So we are that short link or we are that last mile between intelligence that could be operationalized and be worked on by a customer to take a positive action, and we have done that clearly in a number of cases since I came on board in February; not because of me, but I can cite this as an example.

I have lived through—we have informed at least three U.S. carriers about—we will just call them in an open hearing nasty situations in certain parts of the world. We were the ones who took it from the high classified side, worked a story down that is deliverable to the airlines in this case, explained to them the problem in some cases face to face, and then watched them take whatever actions they thought were appropriate. I think that is a more deliverable kind of intelligence that we are responsible to to the transportation industry of America than what I consider the IA approach, if you will, or focus, is very much a strategic and very much completely across the board of homeland defense.

Mr. GIBBONS. Mr. Gaches, are you saying that homeland security doesn't do transportation analysis of its intelligence?

Mr. GACHES. Oh, no, sir, not at all.

Mr. GIBBONS. What you are saying is you are a second set of eyes on the same intelligence or the same analysis that homeland security does?

Mr. GACHES. Sir, I probably misspoke in that what I mean is lots of folks get the same intelligence reports wherever they are derived from. We at TSA will get similar or identical reports as to what DHS IA does and many other people within the community or in the U.S. Government.

What I was trying to say was I think unlike DHS IA, who I have seen tends to take a more strategic across-the-board look at sometimes—a larger look at even a given subject, we are very much more in the tactical—tactical environment with our customer set on a daily basis.

Mr. GIBBONS. Very briefly because my time is limited. From that standpoint, where would you suggest improvement in TSA's analytical intelligence efforts?

Mr. GACHES. I think that we have a lot of room to improve in just the taking a lot of the tactical information that we get, a lot of which comes from the field that TSA is in. In other words, we have two different reports in particular in which TSA officers, wherever they may be in the U.S. system, but as TSA, provides at least 60 percent of the information that comes into us to put those reports together, and I believe that we probably need to take that information and step back just a little bit, not too far, and start to look more at trends in different transportation networks; see if there are patterns, compare across transportation networks and see if there are more similarities between, say, aviation and rail activities, et cetera, still not in that larger assessment role that I see

DHS IA doing, but clearly we have some room to grow in that TSA OI.

Mr. GIBBONS. What keeps you awake at night, Mr. Gaches?

Mr. GACHES. A lot of things in this business after a lot of years. But in all seriousness, sir, a great question. I think right now there are probably two things that I will sort of generalize in an open forum, and that is if you look at London, if you look at what has happened in Canada recently, the phrase comes about that we use "home-grown," and I think that is a that is a field ripe for study and for analysis about home-grown individuals wanting to engage in the terrorist activity as opposed to awaiting the next shipment, if you will, from an overseas location. That certainly is one thing.

The other thing that I find very challenging, and I, in fact— Mr. Chairman and I were speaking about this the other day. I can't find an answer, and it has to do with sometimes the lack of certain types of activity in this country, and you know, we sometimes wonder with what we see overseas, particularly the use of suicide bombers and improvised explosive devices overseas, we certainly wonder and stay up at night questioning about the lack of that in the U.S., and that is what keeps me up. Some of the things we do about that would best be said in a classified session at another time. I would be happy to take that on.

Mr. SIMMONS. Thank you, Mr. Gaches. The Chair recognizes the gentleman are from New Mexico, Mr. Pearce.

Mr. PEARCE. Thank you, Mr. Chairman. Appreciate the testimony and the opportunity to ask questions.

If you were to look at the structure around the intelligence section of TSA, how far do you have to go around the director, administrator in charge, to find somebody with an intelligence background instead of, say, a lawyer or whatever? What is the management structure?

Mr. GACHES. Specifically within TSA'

Mr. PEARCE. Yes.

Mr. GACHES. Thank you, sir, for the question. Of course you know Mr. Hauley, the Administrator, is literally right above me as the Assistant Administrator and Director of Intel, and he is a very, very strong advocate of his entire staff understanding that he wants intel to drive a lot of the decisions, policy formulations and actions taken by TSA as opposed to we are just going to do it because it seems like a good idea. A very strong advocate.

Mr. PEARCE. I didn't ask if he is an advocate, I asked if he has got background.

Mr. GACHES. I am not familiar with Mr. Hauley's background to that degree. I am unaware of it.

Mr. PEARCE. When TSA started 2, 2 1/2 years ago when they first arrived we were asking the same question. You could go for five or six layers without finding anybody but lawyers, so then the administration program began not to be directed so much at outcomes but in processes and legal defenses and things that really in my mind compromised the ability of the program to work to really protect the American people, and instead appeared to have processes to protect the TSA from outside intervention.

Mr. GACHES. Sir, if I may, I have only been there for 4 months but my access to the Administrator is unfettered by any other As-

sistant Administrator or by his Principal Deputy. We start the TSA day off in my area of intel with all of the other assistant administrators and what we call general managers in attendance of a morning briefing. It is an intel briefing.

I think there is a greatly improved presence of intel and intel usage by TSA in the past 4 months. I am impressed by how an organization in which I am a very, very, very small minority, gets an awful lot of attention from all of the elements of TSA.

I hope that helps clarify, but I am optimistic about the way intel is going at TSA at this time in the administrative sense.

Mr. PEARCE. If I were to ask the local sheriffs in my district—I have got a very rural district, right on the southern border of the country—the last time they got any evidence through the channels, the intel channels rather than through the local news or CNN or Fox News, do you think that they would respond that they ever hear from you all, that there is any mechanism to communicate down to the people on the front lines?

Mr. GACHES. Sir, I honestly don't know about literally the local sheriff, but we do push our information as low as the unclassified level. We literally have hundreds of thousands of recipients of those reports that come out on a weekly basis and those are pushed down as far as any of the operational elements at TSA or DHS Central wish to, and if there is an element that is not hearing from us that anyone feels should, I would be more than happy to have that conversation and probably end up providing that information.

Mr. PEARCE. I wonder, a lot of times TSA begins to contemplate how to respond based on projecting the threat and projecting how the threat is going to arrive. Do we really believe that we can project what the terrorists are going to think next? In other words, mostly we respond to what has happened in the past, so today everybody takes off their shoes because of one shoe bomber.

They are not going to come with shoes the next time, they might come with a shirt or something next time. You can follow it from there. But even with a light touch, too, it just seems like the ability to project what is in the terrorist mind is really unusual.

I see my time has expired. You can answer if the Chairman permits.

Mr. SIMMONS. Please.

Mr. GACHES. In an open forum I will be very careful and say there is a lot that we look back over our shoulder. The old adage that history teaches, et cetera, I think applies in this case. I think we are not in the clairvoyant stage, but I think we have some good sense about the future, and I would like to leave it in an open session at that, and I would love to have a classified hearing at greater detail.

Mr. SIMMONS. Thank you.

We are prepared to do a second round if members are so interested, and, if so, I will start with a couple of questions of my own. You have used the word "tactical" as opposed to "strategic" in drawing the difference between TSA intelligence and, let's say, INA at a DHS level. There has also been reference to planning and developing policies, procedures, and applying resources to the problem of the past as opposed to perhaps a current or future threat.

We have put literally billions of dollars into aviation security, we have heard tens of thousands of people, we have got all kinds of equipment and policies and procedures, and anybody who travels in America has encountered those up close and personal. America is airborne, and, as a consequence, that is a legitimate area to focus, especially after 9/11.

I also have concerns about Amtrak and the national passenger rail system, about Metro in the Northeast, and other computer rail systems like BART. We have got pipelines. I believe all of these different systems come within your purview in one form or another.

Focusing specifically on rail, I serve on the Railroad Subcommittee and there is a tremendous lack of rail security personnel, whether it is Amtrak or whether it is the other systems. And I wonder if you could talk for a minute or so on the staffing that you have to focus on the rail target, if you will, and maybe give us a sense of what those risks are, given London, the Spain and Japanese experiences that we have had.

Mr. GACHES. Thank you, Mr. Chairman, for that question. Indeed our analysts are roughly divided across the different modes. They are not all aviation-oriented or one mode over the other, and we do have a few that can go in different directions.

Certainly the lessons of London, Madrid, and, from the nineties, Tokyo, have made it very clear to us that rail and mass transit are areas that we need a lot of attention and, in all honesty, are probably areas that we could even increase our attention in the future.

We are trying very hard to reach out directly from the Office of Intelligence to the rail and mass transit industries, if you will. We are also utilizing other elements of TSA where there are general managers, if you will, as they are called for the different transportation modes to work through them.

As I mentioned before, we have a series of reports that we issue on a weekly basis that talk about suspicious incidents, observations, surveillances, et cetera. Those are flowing back to all of the sectors, to include rail and transport. And as I also mentioned, a lot of that information is gathered, if you will, or observed by TSA individuals, but also can come to us from an Amtrak or another private rail company or whatever the case may be.

Again, we are trying to keep this a fairly tactical level. This is not necessarily something that we are quite ready, nor probably will we be for some time, to go into the large, large assessment; although twice a year for each one of the modes, if you will, of transportation that I articulated in my opening comments, we do prepare a classified and unclassified assessment from what we have seen at the tactical level and we provide that to many people including, DHS IA who can then take it on to even a further level.

So I think we have fairly robust effort with the rail activity. It is one that we are building. I certainly can't say that it is as robust as aviation for some of the obvious reasons that you have articulated in our past, but we are clearly looking at that as an area of future concern in trying to react accordingly and increase our involvement with that sector.

Mr. SIMMONS. Thank you. Very briefly, you spent 30 years with the National Security Agency, one of the key components of the U.S. Intelligence Community, with the CIA, FBI, DIA, the military

services and so on. TSA, as you mentioned, is not one of the 16 members, TSA Intelligence. What motivated you to move from one of the 16, one of the premier, to a relatively small, relatively new, relatively unknown component of intelligence?

Mr. GACHES. Thank you, sir. Small, unknown and those other things, that is a challenge. But in all honesty, d truly I mean this in all honesty and frankness, you can sit outside the DHS family and you can make criticism, or you can join the team and help make it better. I was headed back to NCTC and potentially, probably, retirement. And when Charlie said, would you have any interest in doing this, it was just too good to be true, and I couldn't get down to Arlington, Virginia fast enough.

I find it exciting, challenging, good workforce, dedicated group of folks where homeland focused. In those 30 years—and I mentioned doing counterterrorism at NSA—I spent my fair time doing other things that might not be homeland focused, and it is pretty rewarding to try and apply that knowledge, if I may be so bold as to say there is knowledge to specifically the homeland environment. It was an easy choice, it truly was.

Mr. SIMMONS. Thank you. The Chair recognizes the Ranking Member.

Ms. LOFGREN. Thank you. I want to get back to the terrorist watch list, because as has been discussed here, it is important. We can't get it perfect, I think we know that. We need to do the best that we can. We need to probably err on the side of caution. So I don't think there is disagreement on those basic points.

On the other hand, the GAO has told us that we are—I don't want to say starting over, but going through manually the entire list, and I think TSA and TSC is going through it, but it is going to take 5 or 6 years, according to GAO, to complete that. And it strikes me that that, therefore, means it is a never-ending task because as that review is going through manually, more information is going to be coming in and we will have to go through that manually.

Have you thought about this and what we could do that might make that more efficient and accomplishable in the near term?

Mr. GACHES. Not as much as I probably should, ma'am, to be perfectly honest. I think that there are so many entities now involved in the watch list process that it is probably time for us to once again sit down and examine the roles of the individual agencies, entities, and talk about this very subject of taking so much time to go through this list and revet it. Because you are absolutely correct, we will get through the list. By the time we get to the Zs there will be a whole new group of As, Bs and Cs.

I have no particular straight substantive answer for you except the promise to look at this, to become more involved in this, and, as I said earlier, would really welcome the opportunity to talk to the subcommittee in a classified session with others who are involved in the process, because I could easily misspeak or misinform you by trying to address some of the areas that you have brought up that I think fall outside of my specific office area's responsibility.

Ms. LOFGREN. Let me ask, it is not just the government but it is all of the private sector partners that have to be aligned on one

mission, which is to keep us safe; but the private sector actors are pretty reliant on the information we give them. And it strikes me—I am sure you wouldn't disagree—to the extent that we are stopping babies whose name is Osama, we are wasting our time and effort that should be focused on real threats, and we don't have enough time to spare to divert ourselves for things that don't work.

I was listening to the Chairman talk about the redress committee and I think it is important from an individual's point of view that if you are unable to fly and you are the wrong guy, that you be able to get that fixed. None of us quarrel with that.

What has always bothered me is, once it is fixed, it is important not just for the individual but for the system itself so we don't divert our efforts to things we don't need to look at. So, for example, if you have Sean O'Casey on the IRA and on the watch list, a Sean O'Casey who is complaining that he was born in 1935 and he is not the real guy, somehow that information needs to get into the system so that the airlines cannot waste their time on the older Mr. O'Casey and be looking for the real Mr. O'Casey.

It seems to me we don't have enough data in the system to allow for the corrections itself. Have you thought strategically how to layer that information so that we can actually focus our efforts on the people we are really worried about?

Mr. GACHES. In an open forum I will see if I can give you an answer, ma'am, that makes sense, because I agree with the premise that you just outlined. Because we go from the classified to the unclassified world, there is a fair amount of information that drops off, as you would expect when you get to the unclassified.

I think it would be useful for intelligence officers to step back and see what else could be added to the, quote, unclassified world to make it easier to have the right person stopped, not the wrong person, and also not have the wrong person stopped in the future.

I am not sure that we have even gone down that path, but as you spoke I think you certainly gave me an idea about dropping back on this and looking at what else could be done as identifiers of the individual besides the current paradigm, if you will, and I wouldn't want to go much deeper into those elements.

Ms. LOFGREN. We had a hearing in the last Congress on the fact that name checks alone were not good enough. I realize in some cases the intelligence—we may not have the whole rich amount of intelligence, and maybe that is all we have got, but that is not always the case. Just seems to me we need to build a system that will utilize the data that we do have, just put aside the individual's interests, I don't want to say that is not important, but in our own interest in keeping the country safe. And if we are going to have a watch list that really works, we certainly want to fine-tune that if we are going to use that for rail systems, anything else with a ticket and a name that we might expand.

I see my time is up, but I would just like to close with a request for information either in writing or, if necessary, in a closed session about what technology is being considered by yourself to share the kind of information that you are receiving with our private sector partners in keeping us safe, that would respect the sources and yet get that information out.

I thank the Chairman.

Mr. SIMMONS. In response to that, I would be happy to schedule a follow-up meeting or briefing in a secure environment for any members of the subcommittee or other subcommittees of the full committee who are so interested. And the Chair now recognizes the gentlelady from New York.

Mrs. LOWEY. Thank you, Mr. Chairman, and thank you again, Mr. Gaches. On another area, we have invested billions of dollars in screening passengers, and certainly the Chairman and all of us are happy to take off our shoes or jackets or whatever is necessary to go through the system.

However, airports are allowed to issue SITA badges to those workers who work in the secure areas. They don't have to go through the metal detectors. They work in food catering, they work in the mechanics of the plane. And as I understand it, in fact, it is a fact that they don't have to go through the screening in most situations.

Now as I understand in Europe, at the largest airports, everyone has to go through the screening. At LaGuardia there are over 20,000 SITA badges that have been issued.

Now, in addition, I think it is important to note that the background checks on workers include only criminal background checks and a watch list. They don't ask for the Social Security numbers. So they don't have any identification.

We know what happened, I think it was about 2 years ago at JFK, there were several airport workers that were arrested for smuggling drugs. Could have been explosives instead of narcotics.

Are you concerned about this and what is happening about this? I have to say with all fairness to Mr. Gaches, I understand you are there for 4 months but I have been talking about there for 4 years. And to me it just doesn't make any sense. If European workers have to be screened and go through those metal detectors, seems we should be able to do it here.

By the way, I mentioned LaGuardia, 20,000 SITA badges; San Francisco International, 16,536; in Las Vegas, 21,912; in Hartford Bradley Airport, 4,133. I am sure they are all good, hardworking people, but why shouldn't everybody have to go through the metal detector and could you please comment what you are thinking about doing about it; are you concerned about it; what should be done about it?

Mr. GACHES. Thank you, ma'am. The role of my office in this particular scenario that you have outlined is probably the role that you could really like us to be and hope that we are, and that is that we are pointing out similar concerns and deficiencies which I would like to elaborate upon in perhaps the closed session, that the Chairman will arrange on the no fly and selectee list issues, because there is a similar process, if you will, for transportation workers, the vetting process. It really would be unfair to talk about that.

But what I am saying is we recognize that there is an issue with issuing SITA badges and we understand that there is a differentiation between a SITA worker and the public individual who goes through a different treatment. And we are looking at that and we are looking at what the threats are associated potentially, and in some cases real, in both those scenarios and those populations. But

it would be remiss of me to go into great detail about our action plan or thinking in an open forum, for obvious reasons, but I would welcome the opportunity to walk you through that in greater detail at another time or in written response.

Mrs. LOWEY. I would be delighted to follow up on this, Mr. Chairman, because it seems to me it is like installing an expensive home security system and leaving the back door open. We are happy to go through these metal detectors, but this is an issue I have been talking about for a long time, and you probably can't discuss in this setting whether there is any security threat that could come from an airport worker, could you?

Mr. GACHES. I think that would probably be remiss of me to go into any detail on that. Yes, ma'am.

Mrs. LOWEY. Perhaps I can give you another follow-up question. Is your office doing anything to analyze potential threats from a terrorist who could gain almost unfettered access to airports by obtaining a SITA badge, or is that for a follow-up hearing as well?

Mr. GACHES. Yes and yes. How is that?

Mrs. LOWEY. Maybe you can answer a follow-up question. I know you are only there 4 months. I am just a Member of Congress but I have been concerned about this for years, especially since 9/11, and then after what happened with the arrest at JFK with narcotics, and we know that this is a risk. Have your predecessors been focused on this at all, have they left you any information, or are you just starting from scratch and just became aware of this issue?

Mr. GACHES. No, ma'am. I would say there is a good portion of TSA not represented by my office that worries about the issuance and the processes for the SITA badges specifically, and certainly that has been ongoing work and revisions and improvements to that process are being looked at and worked on. And certainly from an intelligence standpoint, I certainly believe that my predecessor was quite aware of the potential for this area and looked at that and compared all of the available intelligence information that might exist in that particular realm.

Mrs. LOWEY. Mr. Chairman, I know my time is up and I will conclude. Can you give me one reason, possibility, from reviewing this—because this is an important issue—as to why someone with a SITA badge shouldn't have to go through a metal detector, one possible reason? Why wouldn't they? Why wouldn't they give the benefit of the doubt to the possibility of a threat. Why should someone get a SITA badge, not have it reissued for a couple of years, go into a secure area, service the plane, whether it is in food, catering or mechanics, have access to that plane, when you don't have their Social Security number, no one is sure that they haven't passed the badge to someone else? Has anyone recommend that this be changed?

Mr. GACHES. Again, ma'am, I believe that that whole process is being reviewed at this time; the criteria for those badges being reviewed.

Mrs. LOWEY. How long is this review going to take? I have been asking for this review for the last 3 years.

Mr. GACHES. No, ma'am. I apologize. I do not know where they are at in that particular review process. I do think there is a sense

of urgency that has been applied to it just before my arrival, if you will, because clearly it was one of the first issues that I heard outside of the Intel Department of TSA being discussed about in earnest, and our role is to try and contribute some thoughts about if you are going to revise this, what can we the, intel folks, provide to you, the ones that are making the SITA policy; how would you improve it; what are the things you should be looking for, checking for? I kind of leave it at that in open session.

Mrs. LOWEY. Mr. Chairman, perhaps Mr. Gaches could get back to the committee before the next hearing with some kind of time frame. I am still waiting for the Standards—from the Department of Homeland Security—for Interoperability, and I hope we don't have to wait another 3, 4 years for you to conclude this evaluation.

Good luck to you. I know you have only been there for 4 months.

Mr. SIMMONS. I thank the gentlelady for her questions. I agree with the thrust of her comments. And I think we all have that concern, that people who are badged but in and out on a regular basis, sail on through. From my own background and experience, food can be configured in many different ways, not just to eat, but to do other things. And so that can be an issue. Certainly issues relative to mechanics and maintenance are important.

I am not convinced that Mr. Gaches' office is the central focus for this activity, but I would be happy to invite him back to a closed session with other participants to see what the delay is and see what we can do to expedite it.

Mrs. LOWEY. If I may just respond to one thing, my concern here is if Mr. Gaches' office doesn't have the responsibility, who does? My experience is there is a great big bureaucracy out there, and so if you can find the answer to that question, let us now how long this investigation——

Mr. SIMMONS. I think what we will probably find is that site managers probably have substantial discretion, whether they should have it or not. But I feel badly for my colleague from Nevada who has been waiting so patiently, and I now recognize him.

Mr. GIBBONS. Thank you very much, Mr. Chairman, and I will try to not take too long.

I wanted to go into an issue of the area of information sharing, simply because over the last many years there has been a question not so much about agency to agency, although there still is this, I don't know, obstacle between sharing when people want to take pride in their work product and credit for what they do, but information sharing from the Federal level down to the State and local level in transportation issues, whether it is airport, rail, highway, whatever.

Talk to me a little bit about whether or not that information sharing responsibility is through the TSA or only through Homeland Security.

Mr. GACHES. No, sir. It is a combination, and what I mean by that is we view that the DHS IA has a very, very strong charge to work with the State Homeland Security advisors and the local government elected officials and advisors. That does not preclude TSA, who is a strong participant on the transportation side, with two different bodies, if you will, ISACs, which are really the transportation network and private sector companies, if you will, getting

together, whether it is highway or rail or aviation. And those are localized as well as nationalized. They are helping to push information down.

There is also another fairly new adventure with the government councils in which we are trying to facilitate the pushdown of information to State and local transportation authorities, and DHS is working with the Homeland Security advisors; and as long as we are working together with DHS IA, we are trying to ensure that all of the appropriate State and local, be they elected or private individuals involved in transportation, are aware of some version in a form that is useful of threat, new developments. And I harken back to the report that I mentioned that we send out on a weekly basis on both fueled intelligence activities, as we call it, and also suspicious incident reporting. Those are to be shared widely amongst State and local, both government and private sector entities.

I mentioned perhaps earlier that very little of this information should be viewed as so secret that some version of it can't be shared with that furthermost point, and I am certainly interested in trying to solve the sheriff's problem of your colleague, because every time we hear this we are going to find gaps where we are not quite there yet in getting that information out and down. But it certainly is one of the highest goals of the Office of Intelligence at TSA to ensure that happens and that we don't have surprises at the distant end of the system, if you would.

Mr. GIBBONS. I suppose that TSA, then, as well as Homeland Security, have their own protocols for sharing information.

Mr. GACHES. But they are concurrent protocols in how we do that and we do that together.

Mr. GIBBONS. Current, meaning?

Mr. GACHES. The protocol is such that I believe they understand our role with the transportation industries and associated State and local transportation activities. I think we understand their slightly upper-level approach to the State and local government officials. And when I say "protocols," concurrent is probably the wrong word, more "complementary," so that there is coverage for all and not unnecessary duplication across entities from DHS Central, if you will, and from the DHS office.

Mr. GIBBONS. Are there times you have to seek permission or authority from Homeland Security to share information vertically?

Mr. GACHES. We have had occasions where when we have informed DHS Central that we wanted to send something out, they have asked if they could look at it to make it a better informed product. If someone can make it a better informed product at DHS IA, I am willing to do that. We have sent many other things out, including the weekly reports that I have mentioned, and there is no—we have to get permission to do it before we send it.

Mr. GIBBONS. Sometimes States do undertake their own analytical fusion centers. California is doing that, I think Nevada is looking at doing something similar to that as well. Do you actually either have an individual that coordinates or is in place in those fusion centers on the State level that is either trained to look at or to work through your details and your information?

Mr. GACHES. No, sir; we do not. DHS is working with those State fusion centers and Charlie Allen is working on a program, I believe, to have IA intelligence analysts deployed to those State fusion centers. TSA Office of Intelligence, as I have described, is not overly large; appropriately sized for what we are tackling.

But one of the things we are going to experiment with in this year, in fact we started at the beginning of June, is to deploy a TSA Office of Intelligence analyst to six of the Federal security directors who happen to be located at airports. But they are intermodal-thinking people, if you will, and we want to see if there is a value in putting one of our headquarters folks out a little more at the pointy end of the spear, where that individual can do two things for us in a very rough sense: one, make sure the intelligence that TSA Office of Intelligence is producing is being used and being understood at that particular location; and, conversely, those observations, that information which is occurring in that geographic area where that person is assigned again to the TSA Federal Security Director, gets back into my analyst in Arlington so we can be better informed.

We will weigh the pros and cons of that after trying it for 6 to 12 months and see where we go with that in conjunction with what Charlie Allen is doing with his infusion of analysts to the fusion centers of the States.

Mr. GIBBONS. Mr. Chairman, I appreciate the time you have given. There are certainly a number of questions I could have asked, but I will yield to anyone else at this point in time who wishes to ask further questions.

Mr. SIMMONS. I appreciate that. Your time has expired but the Chair is happy to recognize the gentleman from New Mexico for his time.

Mr. PEARCE. Thank you. I thank the gentleman for yielding expired time to me. People do that with parking meters all the time.

If you would explain to me about how you achieve the risk-based security strategy—in other words, what is the quantitative measurement of that risk base, in very short form, because I have 3 or 4 minutes' worth of questions. How do you achieve that internally; how do you look and evaluate the risks?

Mr. GACHES. I wince because it is a great question. At the same time it makes me nervous, I think from my background, to try and give you a solid answer. But let me take a shot. Any of the threats that we are concerned about at any given time are constantly evaluated, and our evaluation compared to others who are evaluating the same risk. As I mentioned earlier, lots of us receive a lot of those initial intel reports to sort of chew on and think about, and that is a good thing, actually, because you don't want just one, if you will, leading the way all the time.

So we look at the veracity of the reporting of the sourcing, et cetera. We do take into consideration the vulnerability of the potential target. We also take into consideration the likelihood of the scenario.

I for one am less concerned at proving the veracity of the likelihood because people can be very inventive, and just because it doesn't make sense to us doesn't mean it hasn't made sense to someone else. So it is a combination of factors that lead us to deter-

mine those three major areas: the sourcing, the vulnerability, and I would also say somewhat along the line of the likelihood of this being a situation that is actually capable of being executed by the adversary.

You add the particulars of those together and it gives you some sense, at least in my opinion, of what the risk is to that potential target.

Mr. PEARCE. That is fair enough. If we look at the sourcing, I would suspect that if we looked in Iraq and we looked at al Qaeda and their past actions, that might be a source. They have had a tendency to blow up refineries and pipelines, then we look at the vulnerability of the pipelines. There are major pipelines running out of New Mexico into California that are significant, in likelihood, again going back to their past actions in Iraq.

I would suspect that TSA has not—and I don't want to make statements in an open meeting—I would just think that they don't get very high on your vulnerability list on your risk assessment. I suspect that pipelines are not in full view. And you can either confirm or say that you can't deal with that.

Mr. GACHES. I would say in this forum, sir, that it probably would be best left to a closed session. But at the same time, I do want to give you a sense, and it is difficult because currently we have concerns about pipelines, and I will be happy to give you those details.

Mr. PEARCE. I appreciate that. Then we were discussing the local sheriffs and the sharing of information, and I will accept that there is probably not much percolation down there. But going to your layered approach, that is, trying to stop the threats as far away as we can, seems like that you would be seeking information from local sheriffs. In other words, the local sheriffs at a meeting told me we routinely have people that have brown skin and black hair that can't speak a word of English or a word of Spanish. They have given themselves a Spanish surname, but the chance is they are really Arabic, and maybe Middle Eastern, coming in. And yet no one seems to care that they are interdicting these people and under the catch-and-release they are back out.

They stopped four or five people with Middle Eastern accents recently; I mean with Middle European. They felt like they were probably from the Soviet Union or something around there. And it doesn't seem that anybody is interested. Do you at least have an e-mail address where these locals out here can share information so that your layered approach can begin to utilize scattered, random sightings or information sources? Do you have something like that?

Mr. GACHES. Sir, I would strongly recommend the connection there, and we do make use of this information and I am personally aware of it being used, if you will. That type of information, that scenario that you just described, really needs to be reported to the Border Patrol and perhaps the Customs, but particularly Border Patrol, because we do get reports of those crossings.

Mr. PEARCE. They called Border Patrol and they told them they are busy, they would check on it tomorrow. I am telling you, the system has broken pretty badly on the border and it seems like at

some point we would really work on passing this information up and down.

I see my time has gone. Thank you very much.

Mr. GACHES. Mr. Chairman, if I may comment, happy is perhaps not the right word, but I will take that concern back and the Border Patrol reaction back to CBP, because we are dependent on them to be the ones who are in fact gathering that information from the local authorities along the border and funneling that into a system that we at TSA can access, and see if that plays into, perhaps in this case, a pipeline issue or another transportation network issue. So I will take that on to get with CBP and hopefully get back to you, sir.

Mr. PEARCE. It may be in transition, but I can tell you in the past there has been almost no desire for information from local law enforcement officers by CBP. And it begins at the interdiction of criminals, and if you are an illegal into Mexico and if you commit an illegal act, you are turned loose because the judge is not going to convict. In fact, they have predescribed limits for illegal drugs. I think it takes 120 pounds of marijuana to reach the threshold where the judge and the system will actually accept the complaint.

So I am just telling you that sitting here in Washington, you may not know how badly the system is disrupted, for whatever purposes. It may be in the process of changing, and I have good strong hope that it is, because we have had just recent visits with Mr. Aguilar. But in the past, it has been this way, up until 2 months ago, when we had a last public meeting of about 30 different local law enforcement officers discussing these various issues, information sharing.

Again, thank you for your indulgence, Mr. Chairman.

Mr. SIMMONS. I want to thank the members of the subcommittee and our panelist, Mr. Gaches, for being here today. You have an important challenge. You have heard some very important concerns expressed from the podium. There will be follow-up to what we have discussed here.

I hear there are going to be votes around 5 o'clock, so we want to get our second panel going. But at the same time, I want to encourage you, Mr. Gaches, to continue to work hard. We are trying to build something here. We are trying to build something that will serve to preserve and protect the safety and security of our citizens, and, at the same time, protect their civil liberties. And this is not easily done. You are charged with an important responsibility. So we wish you all the best in this endeavor and we look forward to our future interactions. And thank you very much for being here today.

Mr. GACHES. Thank you, Mr. Chairman, Ms. Lofgren, members of the subcommittee. And I too look forward to working with you in the future, hoping to answer more questions in other sessions at your leisure. Thank you again.

Mr. SIMMONS. The next panel will be made up of one person, Cathleen A. Berrick, Director of Homeland Security and Justice, at the U.S. Government Accountability Office. I want to thank her for sitting here for several hours and thank her for her accommodation. She is a senior executive with GAO's Homeland Security and Justice team, and in this position she oversees GAO's reviews of

aviation and surface transportation security matters and has developed a broad knowledge of transportation security practices and related Federal policies and Federal and private sector roles and responsibilities.

In the year 2005 she was awarded the William A. Jump Memorial Foundation's Meritorious Award for Exemplary Achievement in Public Administration. Congratulations for that. She has also held previous positions at the Department of Defense and in the U.S. Postal Service.

Welcome. We look forward to hearing your testimony. We will ask you to speak for 5 minutes or so. We have your written testimony for the record and we look forward to hearing what you have to say.

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

Ms. BERRICK. Thank you Mr. Chairman, Ranking Member Lofgren, and members of the committee for inviting me to discuss TSA's Secure Flight program, a program that will match airline passenger information against terrorist watch lists to identify passengers who should be denied boarding or undergo additional security scrutiny prior to boarding a domestic flight.

Secure Flight, which has not yet been fielded, represents a practical application of the use of terrorist watch lists and the impact that intelligence information and its use has on the traveling public. In addition to utilizing terrorist watch lists, Secure Flight will also be supported by intelligence analysts from TSA and the Terrorist Screening Center, who will determine whether potential matches to the watch list are in fact actual matches during the prescreening process.

Currently, prescreening for domestic passengers is conducted by air carriers. Air carriers match passenger information against information contained in TSA's no fly and selectee list, which are provided by TSA prior to passengers boarding a flight. Secure Flight is being developed to take over the prescreening function from air carriers. By taking over this function, TSA will use one common prescreening system for all domestic passengers, rather than each carrier using their own and sometimes differing systems, as is the case today. Secure Flight will also use an expanded terrorist watch list during the prescreening.

My testimony today focuses on the development and oversight of Secure Flight, key factors that will influence the program's effectiveness, and TSA's coordination with key stakeholders who are critical to the program's success. Overall, our work has found that TSA faces significant challenges in implementing Secure Flight, and that the program was at risk in not meeting its goals. Due in part to these issues, TSA announced in February that it was halting development of Secure Flight and was rebaselining the program. During rebaselining, TSA is reassessing the program goals, requirements and schedule, and these efforts are ongoing.

Related to systems development, we found that TSA had not conducted critical activities consistent with best practices for large-scale IT systems. For example, officials declared the design phase

of Secure Flight complete before fully defining system requirements.

We also found that TSA must still make key policy decisions that will influence the program's effectiveness. These decisions include determining what passenger information air carriers will be required to collect to support name matching and how data quality issues with passenger and terrorist watch list information will be mitigated.

These decisions will influence a number of potential matches against terrorist watch lists, the number of passengers who may be inappropriately inconvenienced during the prescreening process, and the ability of the program to appropriately identify individuals actually on the terrorist watch list.

TSA must also determine the level of support needed from TSA's Office of Intelligence and the Terrorist Screening Center to resolve questionable matches of passenger information to terrorist watch lists.

We also found that TSA has collaborated with key stakeholders whose participation is critical to support Secure Flight. However, these stakeholders, to include the Terrorist Screening Center, have stated they need more information about Secure Flight requirements in order to able to support the program.

In light of TSA's rebaselining efforts, two air carriers we spoke with were moving forward with making improvement to their current passenger prescreening system because they stated they were unsure when or if Secure Flight will become operational. While these efforts may improve individual systems, the modifications could result in further differences that already exist among the existing air carriers systems. These differences may result in varying levels of effectiveness in the name-matching process against terrorist watch lists.

Since we testified on these issues in February of 2006, in addition to rebaselining the program TSA has taken several actions to instill more discipline into the development of Secure Flight. We are encouraged by these efforts and believe TSA should not move forward with implementing the programs until these issues are resolved and requirements are defined.

This concludes my opening statement. I will be happy to respond to any questions.

Mr. SIMMONS. Thank you very much for the opening statement.

[The statement of Ms. Berrick follows:]

United States Government Accountability Office

GAO

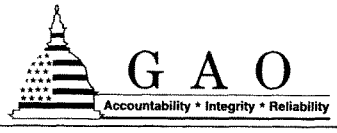
Testimony before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, June 14, 2006

AVIATION SECURITY

Management Challenges Remain for the Transportation Security Administration's Secure Flight Program

Statement of Cathleen A. Berrick, Director,
Homeland Security and Justice Issues



GAO-06-864T

June 14, 2006

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-864T, a testimony before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

After the events of September 11, 2001, the Transportation Security Administration (TSA) assumed the function of passenger prescreening—or the matching of passenger information against terrorist watch lists to identify persons who should undergo additional security scrutiny—for domestic flights, which is currently performed by the air carriers. To do so, TSA has been developing Secure Flight. This testimony covers TSA's progress and challenges in (1) developing, managing, and overseeing Secure Flight; (2) coordinating with key stakeholders critical to program operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing impacts on passenger privacy and protecting passenger rights.

What GAO Recommends

A prior GAO report recommended that the Department of Homeland Security (DHS) direct TSA to take several actions to manage risks associated with Secure Flight's development, including finalizing system requirements, test plans, privacy and redress requirements, and program cost estimates, and establishing plans to obtain data needed to operate the system. DHS generally concurred with GAO's recommendations, but has not yet completed the actions it planned to take. TSA's rebaselining effort is reassessing program goals, requirements, and capabilities.

www.gao.gov/cgi-bin/getrpt?GAO-06-864T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen Berrick at (202) 512-3404 or berrickc@gao.gov.

AVIATION SECURITY

Management Challenges Remain for the Transportation Security Administration's Secure Flight Program

What GAO Found

For over 3 years, TSA has faced challenges in developing and implementing the Secure Flight program, and in early 2006, it suspended Secure Flight's development to reassess, or rebaseline, the program. TSA's rebaselining effort is currently under way, and final decisions regarding the future direction of the program have not been made. In our most recent report and testimony, we noted that TSA had made some progress in developing and testing the Secure Flight program, but had not followed a disciplined life cycle approach to manage systems development or fully defined system requirements. We also reported that TSA was proceeding to develop Secure Flight without a program management plan containing program schedule and cost estimates. Oversight reviews of the program had also raised questions about program management. Secure Flight officials stated that as they move forward with the rebaselined program, they will be following a more rigorous and disciplined life cycle process for Secure Flight. We support TSA's rebaselining effort, and believe that the agency should not move forward with the program until it has demonstrated that a disciplined life cycle process is being followed.

We also reported that TSA had taken steps to collaborate with Secure Flight stakeholders whose participation is essential to ensuring that passenger and terrorist watch list data are collected and transmitted to support Secure Flight. However, key program stakeholders—including the U.S. Customs and Border Protection, the Terrorist Screening Center, and air carriers—stated that they needed more definitive information about system requirements from TSA to plan for their support of the program.

In addition, we reported that several activities that will affect Secure Flight's effectiveness were under way or had not yet been decided. For example, TSA conducted name-matching tests that compared passenger and terrorist screening database information to determine what type of passenger data would be needed for Secure Flight's purposes. However, TSA had not yet made key policy decisions that could significantly impact program operations, including what passenger data it would require air carriers to provide and the name-matching technologies it would use.

Further, Secure Flight's system development documentation did not fully identify how passenger privacy protections were to be met, and TSA had not issued the privacy notices that described how it would protect passenger data once Secure Flight became operational. As a result, it was not possible to assess how TSA is addressing privacy concerns. Secure Flight officials stated that they plan to address privacy issues and finaliz. its redress polices in conjunction with rebaselining the program.

Mr. Chairman and Members of the Committee:

Thank you for inviting me to participate in today's hearing on the Transportation Security Administration's (TSA) intelligence efforts and the integration of its programs that will affect the traveling public, such as Secure Flight. The purpose of Secure Flight is to enable our government to protect the public and strengthen aviation security by identifying and scrutinizing individuals suspected of having ties to terrorism, or who may otherwise pose a threat to aviation, in order to prevent them from boarding commercial aircraft in the United States, if warranted, or by subjecting them to additional security scrutiny prior to boarding an aircraft. The program also aims to reduce the number of individuals unnecessarily selected for secondary screening while protecting passengers' privacy and civil liberties.

My testimony today summarizes the progress TSA has made to develop and implement Secure Flight and the challenges it continues to face as it moves forward with (1) developing, managing, and overseeing the Secure Flight program; (2) coordinating with federal and private sector stakeholders who will play critical roles in Secure Flight operations; (3) addressing key factors that will impact system effectiveness; and (4) minimizing program impacts on passenger privacy and protecting passenger rights. Since I last testified on these issues in February 2006,[1] TSA announced that it was rebaselining the Secure Flight program. This rebaselining effort includes reassessing program goals to be achieved, expected benefits and capabilities, and estimated schedules and costs.

My testimony is based on our March 2005 report,[2] other past reviews of the Secure Flight program (see app. I for a list of GAO products issued on Secure Flight), and preliminary results from our ongoing review of 10 issues related to the development and implementation of Secure Flight, as mandated by Public Law 109-90, and as requested by eight

[1] *GAO, Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T (Washington, D.C.: Feb. 9, 2006).

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

congressional committees.[3] (See app. II for a description of the 10 issues and app. III for additional information on the scope and methodology for this review.) In March 2005, we reported that TSA had made progress in developing and testing Secure Flight, but had not completed key system testing, had not finalized system requirements or determined how certain aspects of the program would operate (such as the basis on which passengers would be selected for preflight scrutiny), and had not clearly defined the privacy impacts of the program. At the time, we recommended that TSA take several actions to manage the risks associated with developing and implementing Secure Flight, including finalizing system requirements and test plans, privacy and redress requirements, and program cost estimates. In February 2006, we testified that TSA had committed to take action based on our recommendations that the agency manage the risks associated with developing and implementing Secure Flight. Although we noted that TSA had made some progress in these areas, we reported that it had not completed any of the actions that were scheduled to be accomplished and long-standing issues related to systems development and testing, program management, and privacy and redress protections remained. Following our February 2006 testimony, TSA announced a temporary suspension of Secure Flight's development to rebaseline the program.

Summary

For over 3 years, TSA has faced significant challenges in developing and implementing the Secure Flight program, a federal passenger prescreening initiative. As we testified in February 2006:

- TSA had not conducted critical development activities, such as following a disciplined life cycle approach for all phases of development, in

[3]Section 518 of the Department of Homeland Security Appropriations Act, 2006 (Pub. L. No. 109-90) requires GAO to report to the Committees on Appropriations of the Senate and House of Representatives on the 10 issues listed in § 522(a) the Department of Homeland Security Appropriations Act, 2005 (Pub. L. No. 108-334), not later than 90 days after the Secretary of the Department of Homeland Security certifies to the above-named committees that Secure Flight has satisfied the 10 issues. These 10 issues relate to system development and implementation, effectiveness, program management and oversight, and privacy and redress. We are also conducting our ongoing review in response to requests from the United States Senate: the Committee on Commerce, Science, and Transportation, and its Subcommittee on Aviation; Committee on Appropriations, Subcommittee on Homeland Security; Committee on Homeland Security and Governmental Affairs; Committee on Judiciary; also the House of Representatives: Committee on Transportation and Infrastructure, Committee on Homeland Security; and the Chairman of the Committee on Government Reform.

accordance with best practices for large-scale information technology programs, potentially putting the program at risk of failure. In addition, TSA had not maintained up-to-date program schedules or developed cost estimates for the program.

- TSA had made progress in coordinating with stakeholders—U.S. Customs and Border Protection (CBP), Terrorist Screening Center (TSC), and air carriers—but additional information and testing were needed before stakeholders could be in a position to provide the support required for Secure Flight to function as intended.

- TSA made some progress in evaluating factors that could influence Secure Flight's effectiveness. However, key policy decisions—such as what data TSA will require air carriers to collect to support Secure Flight operations—and related efforts, to include operational testing, had not been completed.

- Secure Flight's system documentation had not fully addressed how passenger privacy protections were to be met, and therefore potential impacts on privacy could not be assessed. Such an assessment will not be possible until TSA determines, among other things, what passenger data it will require for Secure Flight operations. We further reported that TSA had not yet determined how it would include a process of appeals for travelers erroneously singled out as part of the prescreening process.

TSA has acknowledged these challenges and, based in part on our prior recommendations, has been taking corrective actions. In early 2006, TSA suspended development of Secure Flight and initiated a reassessment, or rebaselining, of the program, to be completed before moving forward. This rebaselining effort is currently under way, and decisions regarding the future direction of the program have not been made. We support TSA's rebaselining effort, and believe that the agency should not move forward with the program until it demonstrates that it is following a disciplined life cycle process.

Background

TSA is responsible for securing all modes of transportation while facilitating commerce and the freedom of movement for the traveling public. Passenger prescreening is one program among many that TSA uses to secure the domestic aviation sector. The process of prescreening passengers—that is, determining whether airline passengers might pose a security risk before they reach the passenger-screening checkpoint—is used to focus security efforts on those passengers that represent the

Transportation Vetting Platform (TVP)[7]—the underlying infrastructure (hardware and software) developed to support the Secure Flight application, including security, communications, and data management and, the Secure Flight application was to perform the functions associated with receiving, vetting, and returning requests related to the determination of whether passengers are on government watch lists. This application was also to be configurable—meaning that it could be quickly adjusted to reflect changes to workflow parameters. In May 2006, TSA officials stated that the agency was considering other approaches for integrating the Secure Flight TVP and application functions in a different configuration as part of rebaselining the program. In its rebaselining effort, this and other aspects of Secure Flight are currently being reviewed, and policy decisions regarding the operations of the program have not been finalized.[8]

Overview of TSA's Plans to Operate Secure Flight as of February 2006

As envisioned under Secure Flight, when a passenger made flight arrangements, the organization accepting the reservation, such as the air carrier's reservation office or a travel agent, would enter passenger name record (PNR) information obtained from the passenger, which would then be stored in the air carrier's reservation system.[9] While the government would be asking for only portions of the PNR, the PNR data could include the passenger's name, phone number, number of bags, seat number, and form of payment, among other information. Approximately 72 hours prior to the flight, portions of the passenger data contained in the PNR would be sent to Secure Flight through a secure network connection provided by

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

[8]The Intelligence Reform and Terrorism Prevention Act of 2004 requires that TSA begin to assume responsibility for the passenger prescreening function within 180 days after the completion of testing. Pub. L. No. 108-458 § 4012, 118 Stat. 3638, 3714-19 (codified as amended at 49 U.S.C. § 44903(j)(2)).

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

DHS's CBP. Reservations or changes to reservations that were made less than 72 hours prior to flight time would be sent immediately to TSA through CBP.

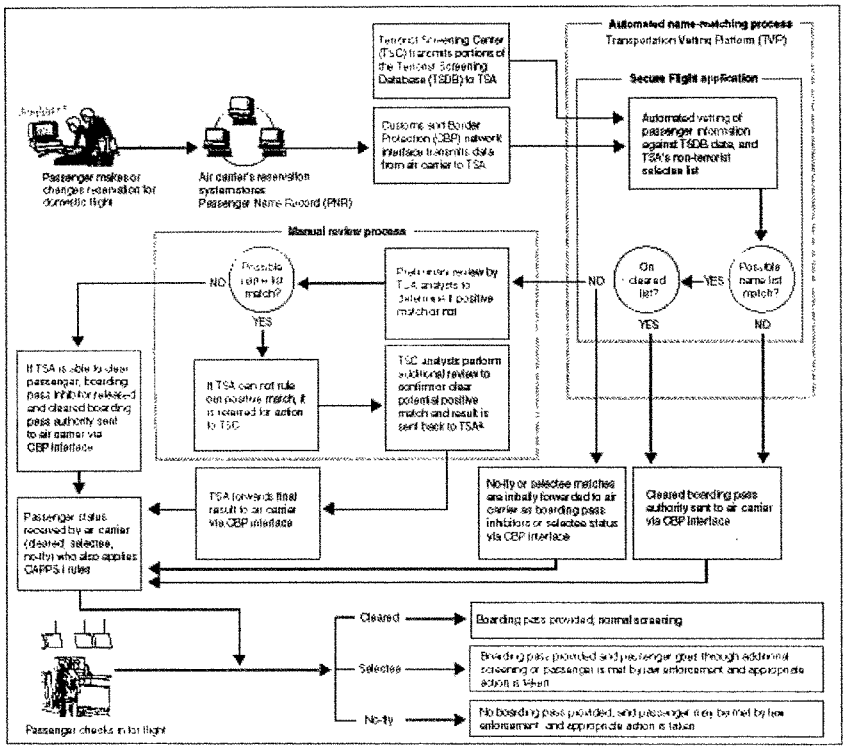
Upon receipt of passenger data, TSA planned to process the passenger data through the Secure Flight application running on the TVP. During this process, Secure Flight would determine if the passenger data matched the data extracted daily from TSC's Terrorist Screening Database (TSDB)—the information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

In order to match passenger data to information contained in the TSDB, TSC planned to provide TSA with an extract of the TSDB for use in Secure Flight and provide updates as they occur. This TSDB subset would include all individuals classified as either selectees (individuals who are selected for additional security measures prior to boarding an aircraft) or no-flys (individuals who would be denied boarding unless they are cleared by law enforcement personnel).[11] To perform the match, Secure Flight was to compare the passenger data, TSDB, and other watch list data using automated name-matching technologies. When a possible match was generated, TSA and potentially TSC analysts would conduct a manual review comparing additional law enforcement and other government information with passenger data to determine if the person could be ruled out as a possible match. TSA was to return the matching results to the air carriers through CBP. Figure 1 illustrates how Secure Flight was intended to operate as of February 2006.

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

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

Figure 1: Planned Operation of Secure Flight as of February 2006



Source: GAO analysis of TSA data.

[a]Information about confirmed no-flys and certain selectees are shared with appropriate federal agencies which coordinate the appropriate law enforcement response.

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

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

As we testified in February 2006, TSA had not conducted critical activities in accordance with best practices for large-scale information technology programs. Further, TSA had not followed a disciplined life cycle approach in developing Secure Flight, in which all phases of the project are defined by a series of orderly phases and the development of related documentation. Program officials stated that they had instead used a rapid development method that was intended to enable them to develop the program more quickly. However, as a result of this approach, the development process had been ad hoc, with project activities conducted out of sequence. For example, program officials declared the design phase complete before requirements for designing Secure Flight had been detailed.

Our evaluations of major federal information technology programs, and research by others, have shown that following a disciplined life cycle management process decreases the risks associated with acquiring systems. As part of the life cycle process, TSA must define and document Secure Flight's requirements—including how Secure Flight is to function and perform, the data needed for the system to function, how various

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

systems interconnect, and how system security is achieved. We found that Secure Flight's requirements documentation contained contradictory and missing information. TSA officials acknowledged that they had not followed a disciplined life cycle approach in developing Secure Flight, but stated that in moving forward, they would follow TSA's standard development process. We also found that while TSA had taken steps to implement an information security management program for protecting Secure Flight information and assets, its efforts were incomplete, based on federal standards and industry best practices. We reported that without a completed system security program, Secure Flight may not be adequately protected against unauthorized access and use or disruption, once the program becomes operational.

Further, TSA had proceeded with Secure Flight development without an effective program management plan that contained up-to-date program schedules and cost estimates. TSA officials stated they had not maintained an updated schedule in part because the agency had not promulgated a necessary regulation requiring commercial air carriers to submit certain passenger data needed to operate Secure Flight, and air carrier responses to this regulation would impact when Secure Flight would be operational and at what cost. While we recognized that program unknowns introduce uncertainty into the program-planning process, uncertainty is a practical reality in planning all programs and is not a reason for not developing plans, including cost and schedule estimates that reflect known and unknown aspects of the program.

Prior to TSA's rebaselining effort of Secure Flight, several oversight reviews of the program had been conducted that raised questions about program management, including the lack of fully defined requirements. DHS and TSA had executive and advisory oversight mechanisms in place to oversee Secure Flight, including the DHS Investment Review Board—designed to review certain programs at key phases of development to help ensure they met mission needs at expected levels of costs and risks. However, the DHS Investment Review Board and other oversight groups had identified problems with Secure Flight's development. Specifically, in January 2005, the Investment Review Board withheld approval of the TVP, which supported Secure Flight operations, to proceed from development and testing into production and deployment until a formal acquisition plan, a plan for integrating and coordinating Secure Flight with other DHS people-screening programs, and a revised acquisition program baseline had been completed. In addition, an independent working group within the Aviation Security Advisory Committee, composed of government, privacy, and security experts, reported in September 2005 that TSA had not

produced a comprehensive policy document for Secure Flight that could define oversight or governance responsibilities, nor had it provided an accountability structure for the program.

TSA has taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, and suspended its development efforts while it rebaselines the program. This rebaselining effort includes reassessing program goals and capabilities and developing a new schedule and cost estimates. Although TSA officials stated that they will use a disciplined life cycle approach when moving forward with the rebaselined program, officials have not identified when their rebaselining effort will be completed.

TSA Had Made Progress in Coordinating with Critical Stakeholders, but More Work Remains

As we testified in February 2006, TSA had taken steps to collaborate with Secure Flight stakeholders—CBP, TSC, and domestic air carriers—whose participation is essential to ensuring that passenger and terrorist watch list data are collected and transmitted for Secure Flight operations, but additional information and testing are needed to enable stakeholders to provide the necessary support for the program. TSA had, for example, drafted policy and technical guidance to help inform air carriers of their Secure Flight responsibilities, and had begun receiving feedback from the air carriers on this information. TSA was also in the early stages of coordinating with CBP and TSC on broader issues of integration and interoperability related to other people-screening programs used by the government to combat terrorism.

Prior to its rebaselining effort, TSA had conducted preliminary network connectivity testing between TSA and federal stakeholders to determine, for example, how information would be transmitted from CBP to TSA and back. However, these tests used only dummy data and were conducted in a controlled environment, rather than in a real-world operational environment. According to CBP, without real data, it was not possible to conduct stress testing to determine if the system could handle the volume of data traffic that would be required by Secure Flight. TSA acknowledged it had not determined what the real data volume requirements would be, and could not do so until the regulation for air carriers was issued and their data management role had been finalized.

All key program stakeholders we interviewed stated that additional information was needed before they could finalize their plans to support Secure Flight operations. Although CBP, TSC, and air carrier officials we interviewed through January 2006 acknowledged TSA's outreach efforts,

they cited several areas where additional information was needed from TSA before they could fully support Secure Flight. Several CBP officials stated, for example, that they could not proceed with establishing connectivity with all air carriers until DHS published the rule—the regulation that would specify what type of information was to be provided for Secure Flight—and the air carriers submitted their plans for providing this information. In addition, a TSC official stated that until TSA provided estimates of the volume of potential name matches that TSC would be required to screen, TSC could not make decisions about required resources.

TSA's ongoing coordination of prescreening and name-matching initiatives with CBP and TSC could impact how Secure Flight is implemented and require stakeholders to alter their plans made to support the program. In January 2006, TSA officials stated that they are coordinating more closely with CBP's international prescreening initiatives for passengers on flights bound for the United States. The Air Transport Association and the Association of European Airlines—organizations representing air carriers—had requested, among other things, that both domestic and international passenger prescreening function through coordinated information connections and avoid unnecessary duplication of communications, programming, and information requirements.[13] In addition, TSC has an initiative under way to, among other things, better safeguard watch list data. At present, TSC exports watch list data to other federal agencies for use in their screening efforts or processes for examining documents and records related to terrorism. However, TSC is currently developing a new system, Query, whereby watch list data would not be exported, but rather would be maintained by TSC. Query would serve as a common shared service that would allow agencies to directly search the TSDB using TSC's name-matching technology for their own purposes. If TSC chooses to implement Query, TSA may be required to modify the system architecture for Secure Flight in order to accommodate the new system.

Due to delays in Secure Flight's development and uncertainty about its future, officials from two air carriers told us after our February 2006 testimony that they were enhancing their respective name-matching systems because they were unsure when and whether TSA would be

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

taking over the name-matching function through Secure Flight.[14] While these efforts may improve the accuracy in each air carrier's individual name-matching system, the improvements will only apply to their respective systems and could further exacerbate differences that currently exist among the various air carriers' systems. These differences may result in varying levels of effectiveness in the matching of passenger names against terrorist watch lists, which was a primary factor that led to the government's effort to take over the name-matching function through Secure Flight.

Key Factors That Could Influence the Effectiveness of Secure Flight Remain to Be Finalized or Resolved

As of February 2006, several activities were under way, or were about to be decided, that would affect Secure Flight's effectiveness. For example, TSA had tested name-matching technologies to determine what type of passenger data would be needed to match against terrorist watch list data. These tests had been conducted using historical data in a controlled, rather than real-world environment, but additional testing was needed to learn more about how these technologies would perform in an operational environment. TSA also had not yet conducted stress testing to determine how the system would handle peak data volumes. Further, due to program delays and the program rebaselining, TSA had not conducted a comprehensive end-to-end testing to verify that the entire system would function as intended, although it had planned to do so by the middle of 2005.

Prior to its rebaselining effort, we further reported that TSA had not made key policy decisions for determining the passenger information that air carriers would be required to collect, the name-matching technologies that would be used to vet passenger names against terrorist watch list data, and thresholds that would be set to determine the relative volume of passengers who are to be identified as potential matches against the database. For example, TSA will need to decide which data attributes air carriers will be required to provide in passenger data to be used to match against data contained in the TSDB, such as full first, middle, and last name plus other discrete identifiers, such as date of birth. Using too many data attributes can increase the difficulty of conducting matching, while

[14] The interviews with officials from the two air carriers is part of on-going work that includes collecting information about name-matching systems currently used by air carriers to match passenger names with those on the no-fly and selectee lists in the TSDB. Information provided by the officials from the two air carriers cannot be generalized to other air carriers.

using too few attributes can create an unnecessarily high number of incorrect matches due to, among other things, the difficulty in differentiating among similar common names without further information. In addition, TSA must determine what type or combination of name-matching technologies to acquire and implement for Secure Flight, as different technologies have different capabilities. For example, earlier TSA PNR testing showed that some name-matching technologies are more capable than others at detecting significant name modifications allowing for the matching of two names that contain some variation. Detecting variation is important because passengers may intentionally make alternations to their names in an attempt to conceal their identities. In addition, unintentional variations can result from different translations of non-native names or data entry errors. TSA had planned to finalize decisions on these factors as system development progressed. However, until TSA completes its program rebaselining, data requirements for the program will remain unknown.

As we reported in February 2006, two additional factors will play an important role in the effectiveness of Secure Flight. These factors include (1) the accuracy and completeness of data contained in TSC's TSDB and in passenger data submitted by air carriers, and (2) the ability of TSA and TSC to identify false positives and resolve possible mistakes during the data-matching process to minimize inconveniencing passengers. Regarding data quality and accuracy, in a review of the TSC's role in Secure Flight, the Department of Justice Office of Inspector General found that TSC could not ensure that the information contained in its TSDB was complete or accurate. To address accuracy, TSA and TSC had planned to work together to identify false positives—passengers inappropriately matched against data contained in the terrorist-screening database—by using intelligence analysts to monitor the accuracy of data matches. Related to the accuracy of PNR data, we reported that TSA had planned to describe the required data attributes that must be contained in passenger data provided to TSA in a forthcoming rule. However, the accuracy and completeness of the information contained in the passenger data record will still be dependent on the air carriers' reservations systems, the passengers themselves, and the air carriers' modifications of their systems for transmitting the data in the proper format. Prior TSA testing found that many passenger data records submitted by air carriers were found to be inaccurate or incomplete, creating problems during the automated name-matching process.

Prior to its rebaselining effort, TSA had also reported that it planned to work with TSC to identify false positives as passenger data are matched

against data in the TSDB, and to resolve mistakes to the extent possible before inconveniencing passengers. The agencies were to use intelligence analysts during the actual matching of passenger data to data contained in the TSDB to increase the accuracy of data matches. When TSA's name-matching technologies indicated a possible match, TSA analysts were to manually review all of the passenger data and other information to determine if the passenger could be ruled out as a match to the TSDB. If a TSA analyst could not rule out a possible match, the record would be forwarded to a TSC analyst to conduct a further review using additional information. Until TSA completes its rebaselining effort, it is uncertain whether this or another process will be used to help mitigate the misidentification of passengers. An additional factor that could impact the effectiveness of Secure Flight in identifying known or suspected terrorists is the system's inability to identify passengers who assume the identity of another individual by committing identity theft, or who use false identifying information. Secure Flight was neither intended nor designed to address these vulnerabilities.

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

TSA is aware of, and plans to address, the potential for Secure Flight to adversely affect travelers' privacy and their rights. However, as we testified in February 2006, TSA, as part of its requirements development process, had not clearly identified the privacy impacts of the envisioned system or the full actions it planned to take to mitigate them. Because Secure Flight's system development documentation did not fully address how passenger privacy protections were to be met, it was not possible to assess potential system impacts on individual privacy protections, as of February 2006. Further, such an assessment will not be possible until TSA determines what passenger data will be required and how privacy protections will be addressed in the rebaselined program.

The Privacy Act and the Fair Information Practices—a set of internationally recognized privacy principles that underlie the Privacy Act—limit the collection, use, and disclosure of personal information by federal agencies.[15] TSA officials have stated that they are committed to meeting the requirements of the Privacy Act and the Fair Information Practices. However, it is not evident how this will be accomplished because TSA has not decided what passenger data elements it plans to

[15]Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. 552a).

collect, how such data will be provided by stakeholders, or how a restructuring that may result from its program rebaselining will impact its requirements for passenger data. Prior to the rebaselining effort, TSA was in the process of developing but had not issued the systems-of-records notice required by the Privacy Act, or the privacy impact assessment required by the E-Government Act, that would describe how TSA will protect passenger data once Secure Flight becomes operational.[16] Moreover, privacy requirements had not been incorporated into the Secure Flight system development process to explain whether personal information would be collected and maintained in the system in a manner that complies with privacy and security requirements. In our review of Secure Flight's system requirements prior to TSA announcing its rebaselining, we found that privacy concerns were broadly defined in functional requirements documentation, which states that the Privacy Act must be considered in developing the system. However, these broad functional requirements had not been translated into specific system requirements. Until TSA determines the relevancy of these requirements and notices, privacy protections and impacts cannot be assessed.

Further, Congress mandated that Secure Flight include a process whereby aviation passengers determined to pose a threat to aviation security may appeal that determination and correct erroneous information contained within the prescreening system.[17] While TSA has not yet determined how it will meet this congressional mandate, it currently has a process in place that allows passengers who experience delays under the current prescreening conducted by air carriers to submit a passenger identity verification form to TSA and request that the agency place their names on a cleared list. If, upon review, TSA determines that the passenger's identity is distinct from the person on a watch list, TSA will add the passenger's name to its cleared list, and will forward the updated list to the air carriers. TSA will also notify the passenger of his or her cleared status and explain

[16] The E-Government Act of 2002 requires agencies to conduct a privacy impact assessment before developing systems that collect, maintain, or disseminate information in an identifiable form. Pub. L. No. 107-347, 116 Stat. 2899.

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

that in the future the passenger may still experience delays.[18] Recently, TSA has automated the cleared list process, enabling the agency to further mitigate inconvenience to travelers on the cleared list. GAO has an ongoing review examining TSA's redress process for assisting passengers misidentified under the screening program.

According to TSA officials, no final decisions have been made regarding how TSA will address redress requirements, but information on the process will be contained within the privacy notices released in conjunction with the forthcoming regulation. In May 2006, Secure Flight officials stated that concerns for privacy and redress were being addressed as part of their rebaselining effort.

Concluding Observations

TSA has recognized the challenges it faces in developing Secure Flight and has undertaken efforts to rebaseline the program. We believe this rebaselining effort is a positive step in addressing the issues facing the program. To make and demonstrate progress on any large-scale information technology program, such as Secure Flight, an agency must first adequately define program capabilities that are to be provided, such as requirements related to performance, security, privacy, and data content and accuracy. These requirements can then in turn be used to produce reliable estimates of what these capabilities will cost, when they will be delivered, and what mission value or benefits will accrue as a result. For Secure Flight, well-defined requirements would provide a guide for developing the system and a baseline to test the developed system to ensure that it delivers necessary capabilities, and would help to ensure that key program areas—such as security, system connectivity, and privacy and redress protections—are appropriately managed.

When we reported on Secure Flight in March 2005, TSA had committed to take action on our recommendations to manage the risks associated with developing and implementing Secure Flight, including finalizing the concept of operations, system requirements, and test plans; completing formal agreements with CBP and air carriers to obtain passenger data;

[18] In our February 2006 testimony, we stated that TSA's Office of Transportation Security Redress (OTSR) managed redress for the current watch list matching process conducted by the air carriers. At that time OTSR was developing an agency-wide policy for redress and had interviewed TSA officials as part of that effort, but found that Secure Flight requirements were not sufficiently defined for use in drafting the new policy. TSA officials stated that they would continue to discuss the Secure Flight redress process with OSTR.

developing life cycle cost estimates and a comprehensive set of critical performance measures; issuing new privacy notices; and putting a redress process in place. When we testified in February 2006, TSA had made some progress in all of these areas, including conducting further testing of factors that could influence system effectiveness and corroborating with key stakeholders. However, TSA had not completed any of the actions it had scheduled to accomplish. In particular, TSA had not developed complete system requirements or conducted important system testing, made key decisions that would impact system effectiveness, or developed a program management plan and a schedule for accomplishing program goals.

In conjunction with its rebaselining effort, TSA has taken actions that recognize the need to instill more rigor and discipline into the development and management of Secure Flight, including hiring a program director to administer Secure Flight and a program manager with information systems program management credentials. We support these efforts and believe that proceeding with operational testing and completing other key program activities should not be pursued until TSA demonstrates that it has put in place a more disciplined life cycle process as part of its rebaselining effort.

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

GAO Contacts and Staff Acknowledgments

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

Other key contributors to this statement were J. Michael Bollinger, Amy Bernstein, Mona Nichols Blake, Christine Fossett, and Allison G. Sands.

Appendix I: Related GAO Products

Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program. GAO-06-374T. Washington, D.C.: February 9, 2006.

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

Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed. GAO-05-356 Washington, D.C.: March 28, 2005.

TSA's Modifications to Rules for Prescreening Passengers. GAO-05-445SU Washington D.C.: March 28, 2005.

Measures for Testing the Impact of Using Commercial Data for the Secure Flight Program. GAO-05-324 Washington, D.C.: February 23, 2005.

Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts. GAO-04-592T Washington D.C.: March 30, 2004.

Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System. GAO-04-504T Washington, D.C.: March 17, 2004.

Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges. GAO-04-385 Washington, D.C.: February 12, 2004.

Appendix II: Legislatively Mandated Secure Flight Issues to be Certified by DHS and Reviewed by GAO

Legislative mandated issue (short title)	Description of mandated issue
Redress process	A system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights by TSA may appeal such decisions and correct erroneous information contained in CAPPS II or Secure Flight or other follow-on/successor programs.
Accuracy of databases and effectiveness of Secure Flight	The underlying error rate of the government and private databases that will be used to both establish identity and assign a risk level to a passenger will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted.
Stress testing	TSA has stress-tested and demonstrated the efficacy and accuracy of all search technologies in CAPPS II or Secure Flight or other follow-on/successor programs and has demonstrated that CAPPS II or Secure Flight or other follow-on/successor programs can make an accurate predictive assessment of those passengers who may constitute a threat to aviation.
Internal oversight	The Secretary of Homeland Security has established an internal oversight board to monitor the manner in which CAPPS II or Secure Flight or other follow-on/successor programs are being developed and prepared.
Operational safeguards	TSA has built in sufficient operational safeguards to reduce the opportunities for abuse.
Security measures	Substantial security measures are in place to protect CAPPS II or Secure Flight or other follow-on/successor programs from unauthorized access by hackers or other intruders.
Oversight of system use and operation	TSA has adopted policies establishing effective oversight of the use and operation of the system.
Privacy concerns	There are no specific privacy concerns with the technological architecture of the system.

Legislative mandated issue (short title)	Description of mandated issue
Modifications with respect to intrastate travel to accommodate states with unique air transportation needs	TSA has, in accordance with the requirements of section 44903 (j)(2)(B) of title 49, United States Code, modified CAPPS II or Secure Flight or other follow-on/successor programs with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger primary selectee status.
Life cycle cost estimates and expenditure plans	Appropriate life cycle cost estimates and expenditure and program plans exist.

Source: GAO.

Appendix III: Scope and Methodology

The results discussed in this testimony are based on our review of available documentation on Secure Flight's systems development and oversight, policies governing program operations, our past reports on the program, and interviews with Department of Homeland Security officials, TSA program officials and their contractors, and other federal officials who are key stakeholders in the Secure Flight program. Throughout our ongoing reviews of Secure Flight, we have reviewed TSA's System Development Life Cycle Guidance for developing information technology systems and other federal reports describing best practices in developing and acquiring these systems. We also reviewed draft TSA documents containing information on the development and testing of Secure Flight, including concept of operations, requirements, test plans, and test results. We also reviewed reports from the U.S. Department of Justice Office of the Inspector General that reviewed the Secure Flight program and reports from two oversight groups that provided advisory recommendations for Secure Flight: DHS's Privacy and Data Integrity Advisory Committee and TSA's Aviation Security Advisory Committee Secure Flight Working Group. We interviewed senior-level TSA officials, including representatives from the Office of Transportation Threat Assessment and Credentialing, which is responsible for Secure Flight, and the Office of Transportation Security Redress, to obtain information on Secure Flight's planning, development, testing, and policy decisions. We also interviewed representatives from the U.S. Customs and Border Protection and Terrorist Screening Center[1] to obtain information about stakeholder coordination. We also interviewed officials from several air carriers and representatives from aviation trade organizations regarding issues related to Secure Flight's development and implementation. In addition, we attended conferences on name-matching technologies sponsored by MITRE (a federally funded research and development corporation) and the Office of the Director of National Intelligence.

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

This testimony includes work accomplished for our March 2005 report[2] and our February 2006 testimony,[3] and work conducted from February 2006 to June 2006 in accordance with generally accepted government auditing standards.

[2]*GAO, Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program,* GAO-06-374T (Washington, D.C.: February 9, 2006).

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

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. SIMMONS. You heard some of the concerns that have been expressed by the subcommittee to the previous panelist and I guess I would be interested in your assessment of the role in the past of TSA Intelligence in cooperating or coordinating with the Secure Flight system and whether you think that role needs to be enhanced, changed in some fashion, or whether we are dealing with a somewhat larger problem involving different entities of TSA and the private carriers.

Ms. BERRICK. Thank you. To answer your larger question, I think we are dealing with a larger problem that I will talk about in a little bit. But with respect to TSA's Office of Intelligence role within the current prescreening process right now, air carriers are doing the actual matching of names against terrorist watch lists. If they conduct a match that is questionable, they don't know whether or not this is in fact a match, they would contact intelligence analysts at TSA to look up additional information to try to determine this person's identity.

If TSA can't make that determination, they will contact the Terrorist Screening Center and the Terrorist Screening Center would help them do that. So that is the intelligence analyst's role right now within the current prescreening process.

Under Secure Flight, intelligence analysts will still need to maintain that role in TSA to resolve potential matches. Although TSA is taking over the actual name-matching function, they will still run into similar situations where they might have a potential match, they are not certain. In those cases, we will need to utilize intelligence analysts within TSA to make that determination, and, again, if they can't make that determination, they will have to work with the Terrorist Screening Center.

But your larger question about this beyond TSA Office of Intelligence' It is. There are some overarching issues with Secure Flight that need to be addressed. Some of you had asked about data quality. That is certainly one important issue both with the Terrorist Screening Center's database, the no fly and selectee list, but also an issue with passenger data, which is the data that is being used to match against the Terrorist Screening Center's database.

There are no standards for collecting passenger data. Each air carrier does it a little bit differently. That greatly influences the effectiveness of the matching process.

Another key factor that can influence how effective these matches are the matching algorithms or software used to conduct the matches. They may try to make a perfect match, as some air carriers do, or some will look for name permutations to try to account for misspellings in names or things along those lines.

So all of those policy decisions have yet to be made in terms of what passenger data will Secure Flight use, what matching algorithms will they use; and all that has the bigger impact, I think, on how effective it will be.

Mr. SIMMONS. What you are saying is that in some respect the approach of the carriers to the problem can affect the efficiency with which the system works. And let me ask you this. I fly Southwest a lot. Let's say there is a hit. Now, do they go back through the system to TSA, to the analyst or to the Terrorist Screening Center, if an automated fashion? Is it something that is relatively

quick because there is connectivity, or do they use telephonic systems or other types of more cumbersome systems? Where are we on that respect?

Ms. BERRICK. It depends on the individual air carrier. Some have better connections than others. But when there is a positive match either to the no fly or selectee list, the air carriers are required to contact TSA and let them know, and TSA in turn will contact the Terrorist Screening Center. So that is in place.

Now, more often than actual matches are questionable matches, and in those cases the air carriers again need to contact TSA, work with the intelligence analyst, and depending on the carrier, that may be electronically, or it may be over the phone. But the more frequent contact is when we have these potential matches that need additional information from TSA on who this individual, is so they can clear them and let them board or take the appropriate action such as calling law enforcement.

Mr. SIMMONS. How effective is the system if somebody buys the ticket at the last minute?

Ms. BERRICK. They are still prescreened under the current process and will be under Secure Flight. It is envisioned, even at the last minute, they would have to get their boarding pass, and go through this process. In addition to this prescreen process, there are other layers of security, as you know, to try to protect aviation security.

You mentioned buying tickets at the last minute. There are other procedures in place that try to augment the current prescreening process that would protect against some vulnerabilities.

Mr. SIMMONS. Thank you. The Chair recognizes the Ranking Member.

Ms. LOFGREN. Thank you. I appreciate your testimony and the report. Rebaselining, does that mean we are starting over?

Ms. BERRICK. What TSA has told us about rebaselining --

Ms. LOFGREN. Is that a word?

Ms. BERRICK. According to our IT folks at GAO they do believe it is a word, and different organizations may define it differently. What TSA has told us is that everything is on the table with the program. They may make changes, they may not. They are going to look at the requirements, look at their goals.

Ms. LOFGREN. So they are starting over pretty much. The question I have is as we are starting over, it is a new opportunity to not make the same mistake over and over again. I was very interested in your comments about what this has been the history of this Department, where they rush off without figuring out what they are doing, and then several years later you have to start all over again. Waste of money, waste of time, and the Nation has been left unprotected.

And it sounds like that is what has happened here again, without the IT systems being defined, you rush off and do it. Same thing happened with the biometrics, how we were going to have consistency. Everybody rushed off and we are going to have to redo that, I am sure ultimately, to the tune of billions of dollars.

The data quality issues and what information is going to be included was not decided upon. And so it seems to me that if you could make some recommendations to us and to the Department

for what could and should be included, that would be enormously helpful.

We got a report in the 108th Congress, I believe, suggesting that names alone were never going to cut it. There needs to be more than just the raw name. And especially in this time of increased identity theft exposure, to use names alone is a huge risk, it seems to me.

So I would appreciate very much if you could tell us right now what your recommendation would be as we start from scratch. That would be useful. And also if you have any information—Mr. Gaches has only been here a short period of time, did not know off the top of his head the technology questions. But do they have access, for example, to those biometrics or do they not' Can you answer those questions?

Ms. BERRICK. In terms of recommendations for TSA as they move forward with Secure Flight, the first recommendation that we have made to them and I would continue to make is that we support this rebaselining effort. We believe they need to establish a disciplined and rigorous development process which hasn't been in place to date. And TSA has stated that they have followed an expedited process in order to field this program quickly. We think they need to slow down to define the requirements and do this more systematically.

In terms of determining what data elements they should be using to support Secure Flight, we think what TSA needs to do is appropriate testing, matching different combinations of passenger data against the watch list to determine what results in the most effective match. TSA has done some limited testing. They have a lot more testing that they need to do before they can make that decision.

And the third point I would make related to TSA moving forward is they need to coordinate with their stakeholders, with the Terrorist Screening Center, with Customs and Border Protection on how this program is going to work and how they are going to support it, and also need to make some key policy decisions that are going to affect this program.

Ms. LOFGREN. Wouldn't there be some simple things to save time' For example, if you have got Sean O'Casey, the IRA guy—if the person before you is 7 years old, that you don't have to go through a big exploration; that the baby is not who you want to stop, or the toddler. I mean, just some baseline things just to clear this out. Couldn't we use common sense like that?

Ms. BERRICK. TSA, Mr. Gaches was mentioning they have a redress office.

Ms. LOFGREN. Not redress, not for the sake of the baby but for the sake of the rest of us; that we are not wasting our time focusing and spinning our wheels about the toddler.

Ms. BERRICK. The quality related to the Terrorist Screening Center database is more, I believe, a TSC issue rather than it is TSA. TSC does have some efforts underway to try to improve the quality. They are doing a record-by-record review. They have some other things in place.

I think it is important that they move forward. As you mention, that will take a while to do. In the meantime, because we are ap-

plying these watch lists today, we want to make sure they are as accurate as they can be. I think the individual agencies have a responsibility to make sure they are doing this responsibly. And in TSA's case, in the case of Secure Flight, I think they can do that by looking at the passenger data that they are getting from air carriers, what are they going to provide them, and coming up with the appropriate mix and software to determine what is going to result in the best match, while separately these data quality issues at the Terrorist Screening Center are being worked.

I think they are both important.

Ms. LOFGREN. I will just close by saying my mother always used to tell me, take your time and do it right, because it is actually quicker than doing it over and over again wrong. Thank you very much.

Ms. BERRICK. Thank you.

Mr. SIMMONS. Your mother was a very smart lady.

Mr. SIMMONS. The chair recognizes the gentleman from New Mexico.

Mr. PEARCE. Thank you.

Do you know what kind of cost has been associated with the Secure Flight program up to this date?

Ms. BERRICK. TSA hasn't been able to identify how much money they have actually spent on Secure Flight and its predecessor programs. We estimate about $120, $130 million but that is an estimate. We don't have an exact figure. TSA estimates are right in that ballpark, too.

Mr. PEARCE. That is close enough. What is your measure of success? In other words, you have got to be—U.S. GAO had to be looking with some parameters to decide that the program is not reaching success. So what is your measure of success?

Ms. BERRICK. We are looking at a lot of areas related to Secure Flight, and we have different criteria for each of those areas. Let us take systems development. We are looking at best practices for the development of IT systems and measuring TSA against that. TSA itself has their own policies for developing major IT systems, and we have looked at, what is their criteria for developing these types of systems?

We found that, in the case of Secure Flight, they weren't following their own systems development guidance. Instead, they had a rapid development approach where some activities were conducted out of sequence. They didn't define requirements, and we believe that was the cause of what has resulted and some of the problems that they are facing right now.

In other areas, for example in privacy and redress, we are looking to what extent they are complying with the Privacy Act, the E-Government Act, fair information principles. So each of these areas we have specific criteria that we are measuring them against, and we are also very open with TSA on what this is. We want to help them be successful and are open with how we are reviewing this program.

Mr. PEARCE. If we go back to that word successful, helping them be successful. Has anyone in the system defined success as something other than compliance' In other words, to me, success would be not knocking down any airliners for a given period of time. So

did TSA set this as an objective evaluation that we are trying to set up a system that will keep us from losing an airliner due to bad passengers doing bad things for the next 7.2 years or something?

Ms. BERRICK. One of the concerns we raised-- and I think your point gets back to requirements-- what do they ultimately want this program to achieve' And we found that, over the 3 years that this program has been in process, the requirements have changed. So it hasn't been entirely clear to us what the goals of the program were.

Now, TSA is saying today that they agree with that. They know that they need to finalize the requirements before moving forward. So, I guess my short answer would be, I don't think the goals have been clearly defined, and they have changed somewhat over time.

Mr. PEARCE. If we are to just take, take the position that it is no aircraft losses due to passenger intervention during the next 10 years, I mean, setting aside spelling of names, algorithms, privacy rights and all that jazz, which has nothing to do with keeping airliners in the air, we are trying to set up a system for expediting passengers. And yet we know in sleeper cells that they sometimes are deactivated, that humans are deactivated for a period of 10 years, 20 years. How in the world can you have a program with all the right algorithms and spellings of names and all that jazz' How can we do this' I mean, it seems ludicrous that we spend the first hundred million dollars not even thinking that we want what we want to achieve, but the fact that we would go ahead and say, okay, just design it right, forget the fact that it can't be done because these people that are willing to do these acts of terror are willing to put backpacks on their kids and stick them in the airplanes and blow them up with I mean, so how why are you suggesting to cure the algorithms when it might not be a curable question?

Ms. BERRICK. I think that is a very good point. Secure Flight is just one specific program of many that TSA has implemented to ensure the security of aviation security, and it is not intended to be the be all, end all. There are many other security layers that TSA pays attention to. So I think it is appropriate to put this in the proper context. It is not intended to do everything. There are other programs in place, but I think that is a very good point, and I agree with that. This is just one program, and it should be viewed in that context.

Mr. PEARCE. What program is set up to stop the 20-year silent nonparticipant and the al Qaeda cell that is waiting to just have his number dialed and say, today's your day' What program is there to stop that person?

Ms. BERRICK. In addition to intelligence, TSA's building in unpredictability into their procedures. For example, in their screening procedures at airports, they are making things a little bit more unpredictable, and that is geared towards the thought that terrorists are going to change their tactics. You may not know what the threat exactly is. This is another tool that they are using to try to get at those types of points where you can't predict where your next threat is, and they have got some other efforts underway, too, along those lines.

Mr. PEARCE. Okay.

Thanks, Mr. Chairman.

Thanks a lot Ms. Berrick.

Mr. SIMMONS. Thank you for those insightful questions. The chair recognizes the lady from New York.

Mrs. LOWEY. I thank you, and I thank you for your presentation and the new vocabulary that you are sharing with us. There was CAPPS I, CAPPS II, now Secure Flight. You say that you think we have spent about $120 to $130 million. I can think of a lot of good uses for $120 to $130 million. The list just gets bigger. There are more errors. Can you give us confidence that as a result of—this is called the rebaseline assessment. Can you give us confidence that if they are rethinking this again, will Secure Flight be any more successful' What directives have you given them' Is it worth even investing the $120 to $130 million' Perhaps you can clarify for me why we, as appropriators, some of us are on this committee, should even think about $120 to $130 million when the agency can't even figure out what they did with the money' And it is puzzling to me how you who are auditing it can even find the money. So should we go ahead with this' I think we are all saying this in different iterations because it is so puzzling.

Ms. BERRICK. Thank you. To first relate it to the benefits of Secure Flight. You asked whether or not we should be moving forward with this.

Mrs. LOWEY. No. No. I think it is important, but do you have any confidence that one strike, two strike, here we go again, that they are going to spend the money any better' Just give us confidence with the directives that you would offer them, that this can be accomplished and at what price?

Ms. BERRICK. Since TSA initiated their rebaselining efforts, we have seen some very positive steps. They brought in new leadership responsible for the program. They brought in people with information systems credentials that they didn't always have prior to that. There has been a commitment from the head of TSA, Kip Hawley, that he really wants to do this right. He wants to slow down. This is an important program. He is going to build this with discipline and rigor. Based on hearing GAO's concerns, Kip Hawley actually initiated an special review of the program, identified the same issues pretty much that we have identified, and that is why they are rebaselining the program. So in terms of the history of this program, I have seen very positive steps lately that are encouraging, and I am looking forward to when TSA completes this rebaselining effort to see how they are going to move forward, but I have seen some very positive actions since the rebaselining was announced.

Mrs. LOWEY. Could you discuss the oversight procedures that have been put in place, so a year from now, you can tell us, yes, they have spent the money, be it— I hate even to think—$100 to $300 million?

Ms. BERRICK. The fiscal year 2006 appropriation legislation requires that GAO report on Secure Flight 90 days after DHS certifies that the system has satisfied its requirements that are spelled out in legislation. So GAO is statutorily mandated to report on the program once TSA certifies that they have met these re-

quirements. So we will be issuing report or testifying on those results at some point in the future after TSA certifies the system, and we are continuing to review the program based on other requests that we have gotten from various committees. So we have a continual presence looking at Secure Flight. After they certify the system, we will be reporting on it.

Mrs. LOWEY. I have found, Mr. Chairman, that as Members of Congress, be it appropriators or not, we look to GAO when all else fails. I guess what I am trying to understand is, do you feel there are appropriate accounting procedures in place as the process moves forward' Or are we going to have to depend on your oversight to make sure that TSA is spending the money appropriately?

Ms. BERRICK. I think there needs to be several oversight mechanisms, and GAO is one. There are also oversight mechanisms at the Department of Homeland Security level. They have an investment review board where they look at these types of programs. They are becoming more involved in Secure Flight. That is a level of oversight. There are also some independent groups that are made up of TSA employees and private sector people that provide advice and counsel to TSA on the program. And in addition, there are often congressional hearings, oversight hearings on Secure Flight and related programs. Most recently before the Senate Commerce Committee in February, TSA and GAO testified on these same issues so. So there seems to be some various mechanisms for oversight, and I think it is important to have all of those as TSA moves forward.

Mrs. LOWEY. Is that same oversight procedure, the same as the one that was in place with the CAPPS I, CAPPS II?

Ms. BERRICK. We were—GAO specifically was mandated to look at CAPPS II. The requirement was a little bit different. That required us to report on the program essentially once every year. It wasn't driven by when TSA certified it. So we were so essentially providing a status update once a year under the old legislation.

Mrs. LOWEY. Well, thank you, Mr. Chairman. I do hope we can get something that is tangible and that works out of this program; $100 to $130 million is a lot of money, and we can think of many uses for it. So thank you very much.

And thank you, Mr. Chairman.

Ms. BERRICK. Thank you.

Mr. SIMMONS. I thank the gentlelady from New York for her continued interest and rigorous oversight activities on these issues. She, like me, shares the memories of 9/11 and probably lost many constituents on that day. So this is something that we all have a deep concern for.

I appreciate your testimony. There will be a follow up on this hearing. We will make an effort to pull together the TSA, the TSC and the CBP into one room, and bring members in and see if we can get our arms around this a little bit, a little bit better.

So I thank all of my colleagues for their participation.

I thank you, Ms. Berrick, for your testimony. Members will have I believe 5–10 working days to submit additional questions and comments for the record. And there being no further business, without objection the committee stands adjourned.

Ms. BERRICK. Thank you, Mr. Chairman.

Mr. SIMMONS. Thank you.

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

○