

United States Department of Homeland Security  
Transportation Security Administration

Statement of Kip Hawley  
Assistant Secretary (Transportation Security Administration)

Committee on Commerce, Science and Transportation  
United States Senate

February 9, 2006

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

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

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

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

### **Secure Flight**

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

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

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

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

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

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

confirmation process and may notify other agencies to initiate an operational response to the match, if appropriate.

We expect that watch list screening under Secure Flight will offer significant improvements in security, efficiency and the passenger experience. It should be noted that any individual who is identified as “no fly” by a government agency is not allowed to board an aircraft under the system in operation today. Nevertheless, security will be enhanced by vetting passengers against the expanded watch lists produced by the TSC, instead of the more limited lists TSA currently transmits to carriers. Further, by moving the watch list screening process within the Federal government, comparisons will be made using a single system, rather than the multiple matching programs now utilized by individual airlines.

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

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

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

In addition to application testing, TSA conducted a separate test to determine whether the use of additional data sources produced by commercial data aggregators could be used to

identify potentially inaccurate or incomplete passenger data and add an additional layer of security in passenger pre-screening. As a result of those tests, commercial data analysis will not be included in the operational deployment of Secure Flight.

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

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

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

### **Registered Traveler**

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

Registered Traveler Pilot programs were initiated in five airports on a staggered basis during the summer of 2004. In partnership with Northwest Airlines, United Airlines, Continental, and American Airlines, TSA established pilot programs at Minneapolis-St. Paul (MSP), Los Angeles (LAX), Houston Intercontinental (IAH), Boston (BOS), and Ronald Reagan Washington National (DCA). Each of the five pilot programs enrolled approximately 2,000 people, who were invited to participate by the airlines from among their very frequent fliers. Participation was limited to U.S. citizens, nationals, and lawful permanent residents, and was entirely voluntary. Participants in these TSA run pilot programs were not charged a fee. The five initial pilots ended in September 2005.

In June 2005, TSA initiated a sub-pilot program at Orlando International Airport (MCO) to test the feasibility of using a public-private partnership model for the program. The

sub-pilot also tests the willingness of the public to pay a fee to participate in a Registered Traveler Program. In the Orlando sub-pilot, participants pay an annual fee of \$80. Approximately 13,000 passengers have enrolled in the sub-pilot, which is still in operation.

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

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

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

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

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

Redress matters will be handled by TSA's Office of Transportation Security Redress until the consolidated traveler screening redress process envisioned by the Rice-Chertoff initiative is developed and implemented. As part of the redress process, applicants

pursuing an appeal may be asked to provide additional information and documents for necessary processing. Applicants will receive the results of their appeal in writing. All Registered Traveler data will be handled in compliance with the Privacy Act.

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

We are fully aware and expect that terrorists may seek to exploit Registered Traveler program benefits, and we are working to design a program to thwart those efforts. Therefore, program benefits can be expected to change from time to time in order to make it difficult for terrorists to anticipate our security activities. In addition, TSA will not exempt Registered Traveler participants entirely from random selection for secondary screening.

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

## **Conclusion**

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

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