

---

## GOVERNMENT AFFAIRS

---

### Fortress America (01/29/2008)

By Michael Milligan

**T**he question of whether a traveler is able to board an airplane may soon be less a matter of available seats, ticket prices or weather conditions and rest more on government consent.

That does not sit well with privacy advocates, many of whom are sounding alarms over the alphabet soup of federal programs introduced since 9/11 to thwart terrorism in the skies and better secure U.S. borders.

To cite just one example, new rules set to go into effect this year require that the name of all passengers buying airline tickets be run through a database to determine if they should be allowed to fly.

Currently, airlines are responsible for vetting passenger names against the government's watch lists when flights are booked. Then Transportation Security Administration officers check to ensure that the name on the boarding pass matches the name on the ID presented at the airport security checkpoint.

#### TSA's 20 levels of security

**T**he TSA has set up these 20 security checkpoints to protect against a possible terrorist attack. The steps start with intelligence gathering and end with the passengers themselves.

- Intelligence
- Customs and Border Protection
- Joint Terrorist Task Forces
- No-fly list and passenger prescreening
- Crew vetting
- Visual Intermodal Protection and Response teams
- Canines
- Behavior-detection officers
- Travel document checker
- Checkpoint/Transportation security officers
- Checked baggage
- Transportation security inspectors
- Random employee screening
- Bomb appraisal officers
- Federal Air Marshal Service
- Federal Flight Deck Officers
- Trained flight crew
- Law enforcement officers
- Hardened cockpit door
- Passengers

But the new program, as proposed, will use a tool known as the Terrorist Screening Database, or the TSDB, to vet passengers. The database is generated by the Federal Bureau of Investigation's Terrorist Screening Center, an entity created by President Bush under a Homeland Security presidential directive.

The FBI describes the TSDB as a "one-stop shopping" program in which "every government screener is using the same terrorist watch list, whether it is an airport screener, an embassy official issuing visas overseas or a state or local law enforcement officer on the street."

The Department of Homeland Security has made the TSDB a key aspect of a program called Secure Flight, one of 20 layers of security designed to operate in concert much "like numbers in a combination lock," in the words of Kip Hawley, head of the TSA, the agency that will be responsible for Secure Flight.

If, for example, a terrorist were to crack the combination for one security layer, Hawley said, he or she conceivably would be tripped up attempting to circumvent another of the remaining 19 layers in order to board an airplane (*see list at right*).

From U.S. land borders and seaports, where 1.1 million passengers and pedestrians are processed each day, to the airports that serve nearly 2 million people daily, the U.S. government is steadily putting in place an array of security programs to better protect U.S. borders by filtering the people and cargo that cross them.

The programs go by different names and have different functions, such as US-

VISIT, an entry/exit program that monitors the arrival and departure of foreign travelers; the Western Hemisphere Travel Initiative, which aims to reduce the documents that may be use for entering or re-entering the U.S. by emphasizing the use of passports; and Electronic Travel Authorization, which will receive advance information on an arriving visitors' travel itineraries and other information.

The overriding objective is to reduce the likelihood of another 9/11-style terrorist attack. Indeed, today's emphasis on security is in stark contrast to the days before Sept. 11, 2001, when 19 al-Qaida terrorists stunned the world by hijacking commercial jetliners to attack the Pentagon and New York's World Trade Center. A fourth plane, hijacked for an attack on the White House, crashed in a field in Pennsylvania as passengers apparently tried to overtake the hijackers.

The 9/11 Commission, which convened three years later to investigate the attacks and the events that contributed to them, noted in its 567-page report that on Sept. 10, 2001, and on all of the days, weeks and years leading up to that time, "border security -- encompassing travel, entry and immigration -- was not seen as a national security matter."

The report went on to make numerous recommendations for improving security. Congress and the White House have since enacted legislation based on the recommendations. And in the years since the attacks, border security has increasingly become a national priority.

"Since 9/11, our nation has put in place critical tools that have strengthened our ability to identify terrorist threats to our homeland, dismantle terrorist cells, disrupt terrorist plots and prevent terrorists from crossing our borders or assuming false identities to carry out attacks," DHS Secretary Michael Chertoff said in testimony before the Senate Committee on Homeland Security on the sixth anniversary of 9/11.

Chertoff said DHS efforts included myriad initiatives in addition to aviation security, such as establishing secure identification, preventing illegal entry across U.S. borders and protecting against dangerous cargo entering the U.S.

"The objective for these initiatives is to try to keep the bad guys out," said Todd Stewart, director of the program for International and Homeland Security at Ohio State University. "But the challenge -- and this is a tough issue -- is how do you keep the bad guys out while welcoming those people who want to come across our borders?"

The Bush administration took a step toward answering that question in January 2006, when Secretary of State Condoleezza Rice and Chertoff unveiled an initiative called "Secure Borders, Open Doors." The initiative was designed to encourage travel, which generates billions of dollars in revenue each year while continuing to shore up security.

Still, a survey of inbound visitors released later in 2006 and conducted on behalf of the travel industry found that many were more fearful of U.S. customs officials than they were of a terrorist attack.

"We are putting up all of these real or perceived walls and barriers, and people get frustrated about whether they can get through the process," said Richard Webster, senior vice president of government affairs for the Travel Industry Association. In the end, he said, U.S. policies dissuade many potential travelers from traveling, particularly by air.

The TIA and most major travel trade groups generally support government efforts to bolster border security, even as they continue to express concerns that the Bush administration may be rushing to put post-9/11 security measures in place before it is ready to execute them.

The WHTI is often cited as a case in point.

Last summer, thousands of Americans were unable to proceed with planned excursions out of the U.S. due to the State Department's inability to accommodate an unprecedented spike in demand for passports generated by the WHTI. The law, which went into effect in January 2007, requires all airline passengers entering the U.S. from Canada, Bermuda, Mexico or the Caribbean (except for Puerto Rico and the U.S. Virgin Islands) to carry valid passports.

The State Department and the DHS, which are responsible for enforcing the WHTI, had planned to extend the passport rule to U.S. land crossings and seaports this summer. But Congress, worried that State and the DHS were moving too quickly, passed legislation that essentially put the land/seaport portion on hold until June 2009.

"Certainly everyone in the industry wants to be part of a secure nation," said Steve Richer, the Washington-based public affairs advocate for the National Tour Association. "However, there are a lot of related issues that don't seem to be directly part of maintaining security, such as slow processing of visa applications, to the point that people decide not to come because of the difficulty in gaining access to the U.S. at various border points of entry."

The travel industry, Richer said, "is looking for a more expeditious type of government security operation."

*CONTINUED...*

<b>Security recommendations of the 9/11 Commission</b>
<ul style="list-style-type: none"> <li>• The U.S. border security system should be integrated into a larger network of screening points that includes transportation systems and access to vital facilities, such as nuclear reactors.</li> <li>• The Department of Homeland Security should complete, as quickly as possible, a biometric entry/exit screening system, including a single system for speeding qualified travelers. Secure identification should begin in the U.S.</li> <li>• The federal government should set standards for issuing birth certificates and other IDs, such as driver's licenses.</li> <li>• The U.S. should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, then develop a plan, a budget and financing.</li> <li>• Improved use of no-fly and "automatic selectee" lists should not await a successor to CAPPs.</li> <li>• The TSA and Congress must give priority attention to improving the ability to detect explosives on passengers.</li> <li>• The U.S. cannot meet its own obligations to protect Americans from terrorists without a major effort to collaborate with other governments.</li> </ul>

*...CONTINUED*

With last summer's passport problems still fresh in people's minds, there are concerns that the government may be heading down a similar path with Secure Flight.

In a notice for proposed rulemaking that appeared in the Federal Register on Aug. 23, 2007, the DHS spelled out the government's

<b>Covert operations</b>
<p>In addition to the highly visible security checkpoints at airports, the Transportation Security Administration has a few less-obvious security measures in place:</p> <ul style="list-style-type: none"> <li>• Visual Intermodal Protection and Response teams: Comprising federal air marshals, surface transportation security</li> </ul>

plans for Secure Flight, which has its roots in a mid-1990s program called the Computer Assisted Passenger Prescreening System, or CAPPS.

Like Secure Flight, CAPPS was designed to prescreen passenger names against the government's terrorist watch lists. It was active in 2001, and according to the 9/11 Commission report, some of the 19 hijackers had been flagged by the CAPPS system. However, at the time, the security paradigm was largely focused on the remote possibility of a hijacker forcing a pilot to fly a commercial airplane to an unscheduled destination, rather than using it in a suicide attack.

Consequently, according to the 9/11 report, "more than half [of the hijackers] were identified for further inspection, which applied only to the their checked luggage."

In the wake of 9/11, an upgraded version of CAPPS, referred to as CAPPS II, was proposed, but it was dogged by privacy-related problems. The government revamped CAPPS again, updating certain components and renaming it Secure Flight.

Under Secure Flight, the TSA will receive information gathered in advance by airlines and, by extension, travel agents for each passenger booked on an airplane.

It will then determine if any of that information matches information on the government's watch lists. If so, the matches will be communicated to aircraft operators.

"Secure Flight will apply to anybody that wants to board an aircraft," said TSA spokeswoman Lauren Wolf. "Once Secure Flight's technology is implemented, watch list matching will be done by the government."

Under the current CAPPS system, "concerns about sharing intelligence information with private firms and foreign countries [kept] the U.S. government from listing all terrorists and terrorist suspects," which increases the likelihood of incorrectly identifying passengers, according to the 9/11 Commission report.

Secure Flight will use only the TSDB, Wolf said, which will create "a more uniform application of the process, improve the passenger experience overall and allow us to better identify individuals who pose a known or suspected threat."

The TSDB is highly guarded, so little is known about it. The FBI has said the database includes information on "both international and domestic terrorists," but beyond that, "its contents are not disclosed."

"All I can say is that individuals known to pose a threat are not allowed to fly," Wolf said. "If you have received a boarding pass, you are not on the no-fly list. It is that simple."

But ASTA contends that it is actually more complicated than that. ASTA, which generally favors Secure Flight, was among more than 500 associations, airlines and individual citizens that filed public comments with the DHS regarding the program.

However, ASTA asserts that the TSA has significantly underestimated the cost and

inspectors, transportation security officers, explosive-detection canine teams and behavior-detection officers, VIPR teams have been in operation for two years, working with local law enforcement to supplement existing security measures.

- Screening Passengers by Observation Techniques: SPOT security officers, deployed in 40 airports nationwide, are trained to utilize "nonintrusive behavior observation and analysis techniques to identify potentially high-risk passengers."

- Federal Air Marshals Service: Armed officers are deployed on commercial airlines and are trained to "blend in with passengers."

- Employee screening: In addition to screening passengers, the TSA last fall began deploying officers to ensure that airport security officers are adhering to procedures.

- Federal Flight Deck Officers: Under this program, certain flight crew members are trained to use firearms, defensive tactics and other procedures to defend against hijackers and other criminal activity on an aircraft. -- **M.M.**

effort for agents and airlines to comply with Secure Flight's requirements.

"If you don't have the mechanism in place, it is not going to happen," said Paul Ruden, ASTA's senior vice president of legal and industry affairs.

Secure Flight requires airlines to transmit the full name, date of birth, gender and certain passport and itinerary information about passengers to the TSA 72 hours before they depart.

As a result, the program will rely on information from the Passenger Name Record, or PNR, that agents and airlines create and store in GDSs.

"We have told the government repeatedly that travel agents are prepared to do their duties," said Ruden. "It was never contemplated that Passenger Name Record would be used to accumulate security information of this kind."

Consequently, the current PNR format cannot accommodate the information that Secure Flight requires, he said.

For example, he said, "There has never been a need for date of birth [in a PNR], so there is no place to put it, except for open text fields. Without those profiles, the [Secure Flight] system doesn't work. So travel agents will have to update those profiles [after the GDSs update the PNR format]."

And that will take time, Ruden said, which in turn could leave millions of travelers in the lurch if the TSA is unable to screen them, especially since it is believed that agencies and airlines will have a short window, possibly as little as three or four months, to comply with the Secure Flight requirements once the final rule on the program is released.

Aside from practical issues, Secure Flight, like many of the government's security initiatives, also raises privacy concerns.

In its comments, the Association of Corporate Travel Executives echoed dozens of others filed by U.S. citizens when it asserted that it was "an individual's right to see what information is in a database that could prevent them from boarding a commercial flight and to change that data if it's incorrect."

The repercussions could be significant: "In the current environment of suspicion, ACTE has determined that being denied access to travel can impact an executive's corporate standing."

Some critics also fear that Secure Flight would prevent thousands of travelers from flying, creating separate classes of flyers and nonflyers.

That could be exacerbated by plans for eventually linking Secure Flight with a Customs and Border Protection program called the Advance Passenger Information System, which focuses on data related to passengers actually seated on airplanes 30 minutes prior to departure.

Rep. Bennie Thompson (D-Miss.), chairman of the House Homeland Security Committee, wrote in comments to the DHS, "There needs to be a uniform process for redress and misidentifications," suggesting that enhancements might be necessary to the Travel Redress Inquire Program, better known as TRIP, the DHS Web-based system for correcting misinformation in its databases.

"Numerous travelers have been ensnared on the TSA's no-fly list and Selectee List, with little knowledge of how to navigate through the redress process," Thompson wrote. "Even air travelers who are aware of the redress process find it difficult."

It is unclear how the DHS will address the issues raised by Thompson, ACTE, ASTA

and others as the department crafts the final rules for Secure Flight, but they lie at the heart of a larger, ongoing policy debate.

"Do we, for example, have to compromise civil liberties and rights of privacy to allow intelligence agencies to get access to communications?" Ohio State University's Stewart asked.

"That is a matter of national choice and balance. I believe -- and I spent 35 years in government -- that people are well intended and trying to do a good job and do the right thing and stay within the law. But again, the national debate is: What is the right balance? What are the trade-offs? ... It is a tough problem."

To contact the reporter who wrote this article, send e-mail to [tweditorial@ntmlc.com](mailto:tweditorial@ntmlc.com).

### Get More!

For more details on this article, see:

- [Making sense of the alphabet soup of U.S. security programs](#)
- [Evolution of the US-VISIT Program](#)

#### DHS gets real about state-issued ids

**T**o reduce document fraud, the Department of Homeland Security has established new standards for state-issued identification cards, including driver's licenses.

Known as the REAL ID program, the new standards require states to incorporate specific information and security features on licenses, requires license applicants to prove their identity and U.S. citizenship or legal status with verifiable source documents and establishes tight security standards for offices that issue licenses and identification cards.

Although secure identification was among the recommendations of the 9/11 Commission, REAL ID remains controversial, with nine states expressing concerns about its cost.

Privacy is also a concern. In a letter to DHS Secretary Michael Chertoff, Rep. Bennie Thompson (D-Miss.), chairman of the House Homeland Security Committee, wrote: "There are myriad privacy concerns raised by the implementation of REAL ID that have not been fully addressed.

"Without adequate institutional safeguards to protect the data contained in the card itself, in the databases that house the information and the facilities that house the databases, the personal identifiable information of the more than 245 million license- and cardholders nationwide is at risk."

States have until Dec. 31 to upgrade their license-issuing systems to ensure REAL ID compliance. They must be able to issue compliant driver's licenses and ID cards to anyone under age 50 by Dec. 1, 2014, and for all other people by Dec. 1, 2017.

The DHS said it was making approximately \$360 million in grants available to assist states with REAL ID implementation.

"The 9/11 hijackers obtained 30 driver's licenses and IDs and used 364 aliases," said Chertoff. "For an extra \$8 per license, REAL ID will give law enforcement and security officials a powerful advantage against falsified documents, and it will bring some peace of mind to citizens wanting to protect their identity from theft by a criminal or illegal alien."

The DHS is also working with several states, including New York, Arizona, Washington and Vermont, to develop "enhanced" licenses that could be used instead of a passport for border crossings. The enhanced licenses would cost more than a standard license and would be embedded with an electronic chip containing additional data. -- **M.M.**

This page is protected by [Copyright](#) laws. Do Not Copy.

Copyright © 2007 by NORTHSTAR Travel Media, LLC. All Rights Reserved.  
100 Lighting Way, Secaucus, N.J. 07094-3626 U.S.A. - Telephone (201) 902-2000