Terrorist Watchlist Checks and Air Passenger Prescreening

William J. Krouse
Specialist in Domestic Security and Crime Policy

Bart Elias
Specialist in Aviation Policy

December 30, 2009

Congressional Research Service
7-5700
www.crs.gov
RL33645

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Considerable controversy continues to surround U.S. air passenger prescreening and terrorist watchlist checks. In the past, such controversy centered around diverted international flights and misidentified passengers. Another issue surfaced on Christmas Day 2009, when an air passenger attempted to ignite an explosive device on a Detroit-bound flight from Amsterdam. Although U.S. counterterrorism officials reportedly had created a record on the air passenger in the Terrorist Identities Datamart Environment (TIDE), which is maintained at the National Counterterrorism Center (NCTC), it does not appear that the NCTC ever nominated him for entry into the U.S. government's consolidated Terrorist Screening Database, which is maintained at the Terrorist Screening Center. Therefore, he would not have been placed on watchlists used by front-line, air passenger prescreening agencies, principally the Department of Homeland Security (DHS), Transportation Security Administration (TSA), and Customs and Border Protection (CBP).

Under Homeland Security Presidential Directive 6, the Terrorist Screening Center (TSC) was established as a multiagency collaborative effort administered by the Federal Bureau of Investigation (FBI). The TSC maintains a consolidated Terrorist Screening Database (TSDB). The TSC distributes TSDB-generated terrorist watch lists to frontline screening agencies that conform with the missions and legal authorities under which those agencies operate. In addition, the TSC has developed comprehensive procedures for handling encounters with known and suspected terrorists and their supporters, and provides terrorist screening agencies with around-the-clock operational support in the event of possible terrorist encounters.

CBP uses the Advanced Passenger Information System (APIS) to capture personal identity and travel information on *international* travelers (both citizens and noncitizens) from passenger manifests provided by air carriers and vessel operators. For the purposes of both border and transportation security, CBP vets that information in most cases prior to departure against several terrorist watchlists that are subsets of the TSDB. More recently, TSA has positioned itself through the Secure Flight program to receive similar data through the DHS APIS portal to vet *domestic* aircraft and vessel passengers against terrorist watch lists, also prior to departure. In time, TSA will assume from CBP transportation security-related terrorist watch list vetting for international aircraft and vessel passengers as well.

In addition, both CBP and TSA capture selected elements of passenger name record (PNR) information that is used to focus inspection and screening resources more efficiently on high-risk individuals at either international ports of entries upon arrival at a U.S. port of entry or at airport security checkpoints prior U.S. air carrier flights. For these purposes, CBP administers the Automated Targeting System-Passenger and TSA administers the Computer-Assisted Passenger Prescreening System. Furthermore, to handle and resolve the complaints of passengers and meet these statutory requirements, the DHS has established the DHS Traveler Redress Inquiry Program (TRIP) as a mechanism for addressing watchlist misidentification issues and other situations where passengers feel that they have been unfairly or incorrectly delayed or denied boarding.

Congress addressed related terrorist watch-listing and screening issues in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) and the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458). In the 111th Congress, the House passed the FAST Redress Act of 2009 (H.R. 559), a bill that addresses air passenger watch list misidentifications.

Contents

Figures

Appendixes

Contacts

Introduction

Considerable controversy surrounds U.S. air passenger prescreening processes and terrorist watchlist checks. On Christmas Day 2009, an air passenger, Umar Farouk Abdulmutallab, allegedly attempted to ignite an explosive device while traveling from Amsterdam on board a Detroit-bound commercial airliner (Northwest Airlines Flight 253). Based on a tip provided by Abdulmutallab's father, U.S. counterterrorism officials reportedly had created a record on Abdulmutallab in mid-November in the Terrorist Identities Datamart Enviornment (TIDE), which is maintained at the National Counterterrorism Center (NCTC).[1] It does not appear, however, that the NCTC ever nominated Abdulmutallab for entry into the U.S. government's consolidated Terrorist Screening Database, which is maintained by the Federal Bureau of Investigation (FBI) at the Terrorist Screening Center. Therefore, he would not have been placed on the Transportation Security Administration (TSA) "No Fly" list or any other watchlist used by other front-line screening agencies. Consequently, this incident has generated questions about "watch-list" procedures. Although those procedures are largely classified, this report provides an overview of recent efforts to improve terrorist watchlist checks and air passenger prescreening.

The incident also raises a new policy issues regarding the interaction between these broader terrorist databases and systems and the "No-Fly" and selectee lists maintained by the Transportation Security Administration (TSA) for prescreening airline passengers, as well as the relationship between passenger prescreening processes and screening procedures to detect explosives and other threat items at airport checkpoints.[2]

Background: HSPD-6 and Terrorist Screening

In September 2003, then-President George W. Bush issued Homeland Security Presidential Directive 6 (HSPD-6), establishing a Terrorist Screening Center to consolidate the U.S. government's approach to terrorist watch-listing and screening.[3] To this end, certain terrorist identification and watchlist functions, which were previously performed by the Department of State's (DOS's) Bureau of Intelligence and Research (INR), were transferred to the newly established Terrorist Screening Center and the Terrorist Threat Integration Center (TTIC)—today the National Counterterrorism Center (NCTC).

NCTC and Terrorist Identification

The NCTC serves as the central hub for the fusion and analysis of information collected from all foreign and domestic sources on international terrorist threats. Under the Intelligence Reform and

[1] Dan Eggen, Karen DeYoung, and Spencer S. Hsu, "Plane Suspect Was Listed in Terror Database After Father Alerted U.S. Officials," *Washington Post*, December 27, 2009, p. A01.

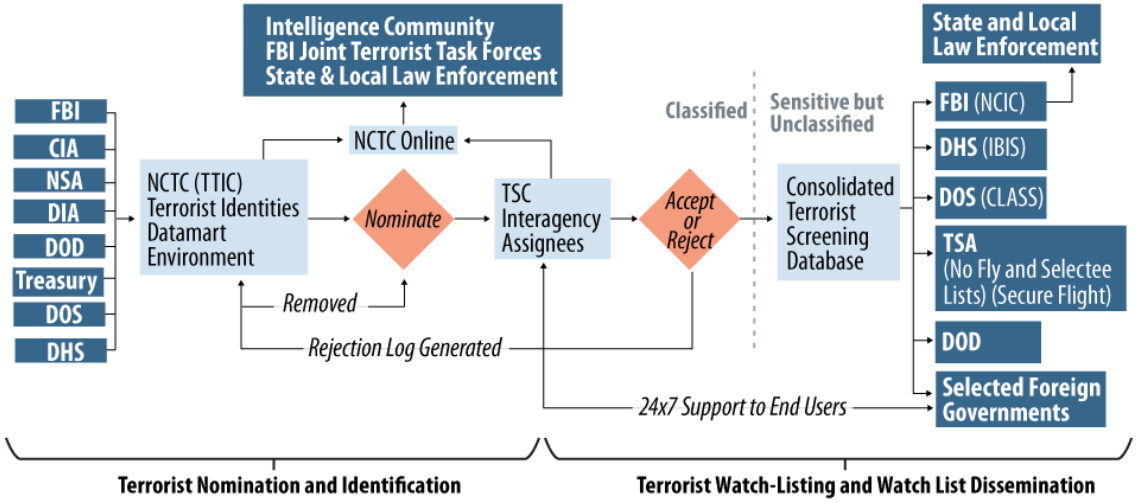
[2] For further information, see CRS Report R40543, *Airport Passenger Screening: Background and Issues for Congress*, by Bart Elias.

[3] The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, September 16, 2003).

Terrorism Prevention Act of 2004 (P.L. 108-458), the NCTC was placed under the newly created Office of the Director of National Intelligence (ODNI). Prior to this legislation and HSPD-6, however, the nation's principal international terrorist watchlist, known as TIPOFF, was maintained by DOS's INR.[4] Under HSPD-6, TIPOFF was officially transferred to the TTIC on September 16, 2003. Nearly a year later, the President established the NCTC by executive order on the foundations of the TTIC.[5] The NCTC continued TTIC's efforts to establish a much more expansive database on international terrorists.

Based partly on TIPOFF, the NCTC currently maintains a Terrorist Identities Datamart Environment (TIDE)—designated under HSPD-6 to be the single repository into which all international terrorist-related data available to the U.S. government are stored. In February 2006, TIDE included over 325,000 terrorist-related records.[6] By August 2008, TIDE had grown to "more than 540,000 names, but only 450,000 separate identities because of the use of aliases and name variants."[7] Less than 5% of those records purportedly pertain to U.S. persons (i.e., citizens or legal permanent residents of the United States).[8]

Figure 1. Terrorist Watch-Listing and Screening Under HSPD-6



Source: Adapted by the Congressional Research Service from a Department of State presentation.

[4] Prior to HSPD-6, INR-generated TIPOFF records were distributed to DOS's Bureau of Consular Affairs (CA), as well as to border screening agencies, for inclusion in the Consular Lookout and Support System (CLASS), the Interagency Border Inspection System (IBIS), and the National Automated Immigration Lookout System (NAILS). For further information, see CRS Report RL31019, *Terrorism: Automated Lookout Systems and Border Security Options and Issues*, by William J. Krouse and Raphael Perl. See also CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by William J. Krouse.

[5] Executive Order 13354, "National Counterterrorism Center," 69 *Federal Register* 53589, Sept. 1, 2004.

[6] Walter Pincus and Dan Eggen, "325,000 Names on Terrorism List: Rights Groups Say Database May Include Innocent People," *Washington Post*, February 15, 2006, p. A01.

[7] National Counterterrorism Center, Terrorist Identities Datamart Environment (TIDE), August 2008.

[8] Ibid.

An effective watchlist process is contingent on Intelligence Community[9] agencies sharing information on known and suspected international terrorists and their supporters with NCTC and, in turn, the NCTC nominating those persons for inclusion in the U.S. government's consolidated terrorist screening database (see **Figure 1** above).

TSC and Terrorist Watch-Listing and Screening

For the purposes of watch-listing, the FBI-administered Terrorist Screening Center (TSC) maintains the consolidated Terrorist Screening Database (TSDB). The NCTC provides international terrorism data and the FBI provides domestic terrorism data for inclusion in the TSDB. Both sets of data are merged in the consolidated TSDB maintained by the TSC. According to the FBI, international terrorists include those persons who carry out terrorist activities *under foreign direction*. For this purpose, they may include citizens or noncitizens, under the rationale that citizens could be recruited by foreign terrorist groups. Or noncitizens (aliens) could immigrate to the United States and naturalize (become citizens), having been unidentified terrorists before entry, or having been recruited as terrorists sometime after their entry into the United States.

By comparison, domestic terrorists *are not under foreign direction* and operate entirely within the United States. According to the Administration, both sets of data (on international and domestic terrorists) will include, when appropriate, information on "United States persons."[10] Criteria for the inclusion of U.S. persons in the database was developed by an interagency working group. The term "United States persons" includes U.S. citizens and legal permanent residents (immigrants). In June 2005, DOJ OIG issued an audit, reporting that the TSC had established a single consolidated TSDB, as recommended by GAO,[11] but with some difficulties.[12] Among other things, the TSDB had not been completely audited to ensure that its records were complete and accurate.

As of September 2008, the TSDB contained 400,000 individual identities, of which 3% are U.S. persons.[13] Due to aliases and name variants, however, the TSDB includes over one million

[9] The Intelligence Community includes the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); the National Geospatial-Intelligence Agency (GIA); the National Reconnaissance Office (NRO); the other DOD offices that specialize in national intelligence through reconnaissance programs; the intelligence components of the Army, Navy, Air Force, and Marine Corps, the FBI, the Department of Energy, and the Coast Guard; the INR at the DOS, the Office of Intelligence and Analysis at Department of the Treasury, and elements of the DHS that are concerned with the analyses of foreign intelligence information (50 U.S.C. §401a(4)).

[10] The definition of "United States person" is found at 50 U.S.C. §1801(i): a citizen of the United States, an alien lawfully admitted for permanent residence (as defined §1101(a)(2) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States, but does not include a corporation or an association that is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

[11] U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO Report GAO-03-322 (April 2003).

[12] U.S. Department of Justice, Office of the Inspector General, Audit Division, *Review of the Terrorist Screening Center*, Audit Report 05-27, (Washington, June 2005), 160 pp.

[13] Written Statement of Rick Kopel, Principal Deputy Director, Terrorist Screening Center, Before the House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, September (continued...)

records on those individuals.[14] The TSC distributes TSDB-generated terrorist watchlists to frontline screening agencies that conform with the missions and legal authorities under which those agencies operate. Consequently, these watchlists (e.g., the TSA's No Fly and Automatic Selectee lists) are in some cases only subsets of the TSDB.

In addition, the TSC has developed comprehensive procedures for handling encounters with known and suspected terrorists and their supporters, and provides terrorist screening agencies with around-the-clock operational support in the event of possible terrorist encounters. For example, TSDB-generated lookout records were and are currently being disseminated to state, local and tribal law enforcement officers through the National Crime Information Center (NCIC, see **Figure 1** above). The unclassified portion of some, but not all, TSDB-generated lookout records (name, date of birth, passport number, and country of origin) are loaded into the NCIC's Violent Gang and Terrorist Offender File (VGTOF). Similar look out records are also shared with the Department of Defense and selected foreign governments. In addition, the TSC supports the terrorist screening activities of TSA and U.S. Customs and Border Protection (CBP), as well as the Department of State's Bureau of Consular Affairs (CA).

9/11 Commission and Integrated Terrorist Travel Strategy

In July 2004, the National Commission on Terrorist Attacks upon the United States (9/11 Commission) made air passenger prescreening- and terrorist travel-related findings and recommendations in its final report. Shortly thereafter, the TSA unveiled the "Secure Flight" domestic air passenger prescreening program (described below),[15] and the Administration issued Homeland Security Presidential Directive 11 (HSPD-11), calling for "comprehensive terrorist-related screening procedures."[16]

Among other things, the 9/11 Commission concluded that disrupting terrorist travel was as powerful a weapon as targeting their money.[17] The 9/11 Commission found, however, that prior to the 9/11 attacks, the intelligence community did not view watch-listing as integral to intelligence work.[18] To prevent future terrorist attacks, the 9/11 Commission recommended that the United States expand terrorist travel intelligence and countermeasures,[19] and that the U.S. border security

(...continued)

9, 2008, p. 4.

[14] Ibid.

[15] U.S. Department of Homeland Security, Transportation Security Administration, "TSA To Test New Passenger Pre-Screening System" (Washington, August 26, 2004), 2 pp.

[16] The White House, *Homeland Security Presidential Directive/HSPD-11, Subject: Comprehensive Terrorist-Related Screening Procedures* (Washington, August 27, 2004).

[17] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, (Washington, 2004), p. 385.

[18] National Commission on Terrorist Attacks upon the United States, "Three 9/11 Hijackers: Identification, Watchlisting, and Tracking," Staff Statement no. 2, (Washington, 2004), p. 1.

[19] *The 9/11 Commission Final Report*, p. 385.

systems be integrated with other systems to expand the network of screening points to include the nation's transportation systems and access to vital facilities.[20]

To increase aviation security, the 9/11 Commission recommended that Congress and TSA give priority to screening passengers for explosives.[21] At a minimum, the 9/11 Commission recommended that all passengers referred to secondary screening be thoroughly checked for explosives.[22] Arguably, this necessitates a robust process to carefully select only those passengers believed to pose the greatest risk to aviation security, while minimizing false positives. To improve air passenger prescreening, the 9/11 Commission recommended that

- the "no-fly" and "automatic selectee" watchlists used to screen air passengers be improved without delay;
- the actual screening process be transferred from U.S. air carriers to TSA;
- air passengers be screened against the larger set of U.S. government watchlists (principally the TSDB); and
- air carriers be required to supply the needed information to test and implement air passenger prescreening.[23]

As described below, both the Administration and Congress acted to implement the 9/11 Commission's recommendations and establish an integrated strategy to disrupt terrorist travel, but the results to date have been mixed.[24]

CBP and TSA and International Air Passenger Prescreening

At air and sea ports of entry, CBP uses the Advanced Passenger Information System (APIS) to capture personal identity and travel information on international travelers (both citizens and noncitizens) from passenger manifests provided by air carriers and vessel operators. For the purposes of both border and transportation security, CBP vets that information in most cases prior to departure against several terrorist watchlists that are subsets of the TSDB. In addition, both CBP and TSA capture selected elements of passenger name record (PNR) information that is used to focus inspection and screening resources more efficiently on high-risk individuals at either international ports of entries upon arrival at a U.S. port of entry or at airport security checkpoints prior U.S. air carrier flights. For these purposes, CBP administers the Automated Targeting System-Passenger and TSA administers the Computer-Assisted Passenger Prescreening System.

---

[20] Ibid., p. 387.

[21] Ibid., p. 393. Also, for further information, see CRS Report RS21920, *Detection of Explosives on Airline Passengers: Recommendation of the 9/11 Commission and Related Issues*, by Dana A. Shea and Daniel Morgan.

[22] Ibid., p. 393.

[23] Ibid.

[24] Jonathan Alter, "Plugging Holes in the Skies: The Terrorists Used Airplanes as Weapons in 9/11. So Why Haven't We Made Travel Safer by Now?" *Newsweek*, August 21-28, 2006, p. 50.

Under current practice, airlines transfer manifest data through CBP's APIS several times prior to departure as it becomes available; however, final advanced passenger information (API) data were sometimes not transferred until after the flight has departed (wheels up). In several cases, known and suspected terrorists have been allowed to board aircraft at airports abroad and, subsequently, this led to costly diversions when air carriers were prevented from entering U.S. airspace or continuing to their destinations. Several of these incidents generated significant press coverage in 2004.[25] As described below, CBP issued new regulations (effective February 18, 2008) that require all international air carriers and vessel operators to provide CBP with API data in advance of an aircraft's departure.

More recently, TSA has positioned itself through the Secure Flight program to receive similar data through the DHS APIS portal to vet *domestic* aircraft and vessel passengers against terrorist and other watchlists, also prior to departure. As originally conceived, the Secure Flight program included an element to select passengers for greater screening at passenger checkpoints based on certain characteristics gleaned from API and PNR data. This element of Secure Flight was modeled to some extent on a controversial program known as the Computer-Assisted Passenger Prescreening System (CAPPS), but is similar to CBP's Automated Targeting System (ATS). Both systems are described below. Although TSA has scrapped this element from its Secure Flight plan, there are no plans to discontinue CAPPS. In addition, under the Secure Flight program, TSA will assume from CBP in time transportation security-related terrorist watchlist vetting for *international* aircraft and vessel passengers as well.

CBP's National Targeting Center (NTC) confers with TSC representatives to resolve potential watchlist matches. Despite close cooperation between CBP's NTC and the FBI-administered TSC, as has been the case for TSA and domestic flights, CBP misidentifications on international flights have also generated some controversy.[26] Despite these difficulties, the 9/11 Commission made several recommendations to increase such data sharing and strengthen air passenger prescreening against TSC-maintained watchlists. Some of these were reflected in provisions that Congress included in the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458). The air passenger prescreening provisions in this law are discussed generally below.

CBP and Advanced Passenger Information System (APIS)

CBP administers APIS to allow international air carriers and vessel operators to transmit data collected from aircraft and ship manifests on passengers and crew members in an electronic format to the CBP Data Center. API data includes both personal identity information and other travel information. Personal identity information is usually collected electronically by air carriers and vessel operators, as well as travel agents, from the Machine Readable Zone (MRZ) on a person's passport or other travel document. It includes, but is not limited to, a person's full name, date of birth, gender, country of residence, and country of citizenship. Additional travel data

[25] See David Leppard, "Terror Plot To Attack US with BA Jets," *Sunday Times* (London), January 4, 2004, p. 1; Sara Kehaulani Goo, "Cat Stevens Held After DC Flight Diverted," *Washington Post*, September 22, 2004, p. A10; and "US-Bound Air France Flight Diverted Due to Passenger," *Agence France Presse*, November 21, 2004.

[26] Niraj Warikoo, "Doctor Says He's Profiled At Airports: Beverly Hills Man Joins Class Action vs. Government," *Detroit Free Press*, June 20, 2006. Jeff Coen, "ACLU Expands Profiling Lawsuit," *Chicago Tribune*, June 20, 2006, p. C6.

elements are also collected from passenger and crew manifests. Those travel data elements include carrier code, port of first arrival, status on board an aircraft or vessel, data and time of arrival, and foreign port code. For a complete list of API data elements, see **Appendix A**.

Through the Treasury Enforcement Communications System (TECS),[27] CBP cross-references API data against law enforcement, customs, and immigration screening systems/databases, as well as terrorist watchlists that have been exported from the U.S. government's consolidated TSDB.

Terrorist Watchlist Checks and Post 9/11 Statutory Mandates

Prior to the 9/11 attacks, API data were collected voluntarily to streamline and expedite the clearance process for law-abiding passengers at international ports of entry. [28] Following those attacks, however, the collection and transmission of API data was mandated under both the Aviation Transportation Security Act of 2001 (ATSA)[29] for commercial passenger flights arriving in the United States and the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA) for flights and vessels arriving in and departing from the United States.[30] In line with the recommendations of the 9/11 Commission, Congress included in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) several provisions related to terrorist watchlist screening. Those provisions require

- DHS to perform preflight terrorist watchlist screening for all passengers and crew onboard aircraft bound for or departing from the United States (Section 4012(a)(6));
- TSA to screen preflight all passengers and crew on domestic flights (Section 4012(a)(1)); and
- DHS to conduct watchlist screening for passengers and crew on cruise ships and other ocean-going vessels (Section 4071).[31]

APIS Pre-departure/Pre-arrival Final Rule

Effective on February 18, 2008, all international air carriers and vessel operators are required to provide CBP with API data in advance of an aircraft's departure or vessel's departure/arrival, depending on the vessel's port of origin (U.S. or foreign).[32] Air carriers have two methods for

---

[27] In the APIS System of Records Notification (SORN), DHS described TECS as an "Information Technology platform." See U.S. Department of Homeland Security, Privacy Office, "Privacy Act of 1974; Customs and Border Protection Advanced Passenger Information System Systems of Record," 73 *Federal Register*, pp. 68435-68439, November 18, 2008.

[28] In 1988, the legacy U.S. Customs Service developed APIS as a module of TECS, in cooperation with the legacy Immigration and Naturalization Service.

[29] P.L. 107-71; November 19, 2001; 115 Stat. 597; Section 115.

[30] P.L. 107-173; May 14, 2002; 116 Stat. 543; Section 402.

[31] P.L. 108-458; December 17, 2004; 118 Stat. 3638.

[32] U.S. Department of Homeland Security, Bureau of Customs and Border Protection, "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels," Final rule, 72 *Federal Register*, pp. 48320-48353, August 23, 2007.

providing this information: (1) "APIS 30" allows operators to submit passenger and crew manifests in batch form by an interactive or non-interactive method no later than 30 minutes prior to securing aircraft doors for departure; (2) "APIS Interactive Quick Query" allows transmission of manifest information as each passenger checks in, up to, but no later than, the time aircraft doors are secured. In line with best practices, air carriers are also encouraged to transmit available APIS data 72 hours prior to a flight. For sea-and ocean-going vessels departing the United States, vessel operators are required to transmit API data 60 minutes prior to departure. For vessels departing foreign ports that are destined for U.S. ports, vessel operators are required to transmit API data no less than 24 hours before arrival and no greater than 96 hours before arrival.

DHS issued a privacy impact assessment for APIS on August 8, 2007.[33] API data for all persons are copied to the Border Crossing Information System (BCIS). For noncitizens, API data are copied to the Arrival and Departure Information System (ADIS) as part of the US-VISIT requirements.[34] Both systems are modules that reside on TECS.

CBP and the Automated Targeting System (ATS)

Given the volume of people and goods seeking entry into the United States every year, it is impractical to physically inspect every person or shipment that arrives at a U.S. port or entry.[35] Therefore, in the mid-1990s, the legacy U.S. Customs Service developed a decision support tool known as the Automated Targeting System (ATS) to assist border inspectors with interdicting illegal drugs and other contraband.[36] Prior to the 9/11 attacks, the scope of ATS was reportedly limited to parties (custom brokers, freight forwarders, and trucking/shipping companies) and cargoes that were associated with past criminality that raised the suspicions of customs authorities.[37] After the 9/11 attacks, ATS was reconfigured and its scope widened to target known and suspected terrorists and terrorist activities as well, by assigning risk assessments to conveyances and cargo, and selecting passengers for enhanced screening.[38]

---

[33] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Advance Passenger Information System (APIS)*, August 8, 2007, 23 pp.

[34] DHS has developed the US-VISIT program to more accurately identify and screen non-citizen border-crossers. Congress first mandated that the former Immigration and Naturalization Service (INS) implement an automated entry and exit data system that would track the arrival and departure of every alien in §110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA; P.L. 104-208). The objective for an automated entry and exit data system was, in part, to develop a mechanism that would be able to track nonimmigrants who overstayed their visas as part of a broader emphasis on immigration control. Following the September 11, 2001 terrorist attacks, however, there was a marked shift in priority for implementing an automated entry and exit data system. While the tracking of nonimmigrants who overstayed their visas remained an important goal of the system, border security and the identification of potential terrorists have become the paramount concerns with respect to implementing the system.

[35] In FY2008, at 327 ports of entry, CBP processed 409 million pedestrians and passengers, 121 million conveyances, and 29 trade entries. CBP also collected approximately $34.5 billion in revenue, apprehended 723,825 aliens attempting to enter the United States illegally, and seized nearly 3.1 million pounds of illegal narcotics. Source: CBP, *Performance and Accountability Report, FY2008*, December 4, 2008, p. 6.

[36] CBP briefing provided to CRS on November 24, 2008.

[37] Ibid.

[38] Ibid.

ATS Modules

Today, CBP's NTC uses ATS to analyze trade data and cargo, crew, and passenger manifest information to "target" its inspection resources toward persons and cargo shipments that potentially pose the highest risk. The NTC was established in November 2001 with the primary mission of providing "round-the-clock tactical targeting and analytical support for CBP's counterterrorism efforts."[39] At the NTC, intelligence from other federal agencies, in the form of "lookouts," and other law enforcement and intelligence reporting are also reviewed. ATS consists of six modules that include

- ATS-Inbound for importers, cargoes, and conveyances (rail, truck, ship, and air);
- ATS-Outbound for exporters, cargoes, and conveyances (rail, truck, ship, and air);
- ATS-Passenger for passengers and crew entering and departing the United States (air, ship, and rail);
- ATS-Land for vehicles and persons entering the United States at land border ports of entry;
- ATS-International for information sharing and cargo targeting with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity for selective targeting based on trend analysis.[40]

With the exception of ATS-Passenger, these modules employ weighted rule sets to assign scores, identifying high-risk conveyances and cargo shipments.[41] Above a certain threshold risk score, conveyances and cargo are subject to further inspection at international ports of entry. [42]

Passenger Name Records and ATS-P

In the air and sea passenger environment, CBP requires international air carriers and vessel operators to transmit passenger name record (PNR) data to the NTC. Like API data, PNR data are collected by air carriers and vessel operators in their automated reservation or departure control systems. Although there is some overlap between the API and PNR data, most PNR data would not be included typically on a passenger or crew manifest. While PNR data have been submitted voluntarily by air carriers since 1997, CBP reports that it collects these data currently as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (P.L. 107-71).[43] PNR data includes, but is not limited to, date of reservation/ticket issuance, dates

[39] National Counterterrorism Center, *National Strategy to Combat Terrorist Travel*, May 2, 2006, p. 28.

[40] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System*, August 3, 2007, p. 7.

[41] Ibid.

[42] National targeting thresholds are set by the NTC and are constantly evaluated and adjusted in response to intelligence and analysis.

[43] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System*, August 3, 2007, p. 3.

of intended travel, payment and billing information, travel agency/travel agent, baggage information, and PNR specific travel itinerary. On July 26, 2007, after considerable negotiations, the European Union and the United States reached a permanent agreement, under which 19 types of PNR data are being collected.[44] PNR data is to be maintained by CBP for seven years in an active file and eight years thereafter in a dormant file.[45] According to then-Secretary Michael Chertoff, DHS has agreed to data protections that meet the privacy standards of both the European Union and United States.[46] For a complete list of PNR data elements under the EU-U.S. agreement, see **Appendix B**. For an overview of the events leading up to this agreement, see **Appendix C**.

Through the ATS-Passenger, CBP compares and analyzes PNR data by comparing it to several law enforcement, customs, and immigration systems/databases that include, but are not limited, to the following:

- Advanced Passenger Information System (APIS),
- Nonimmigrant Information System (NIIS),
- Suspect and Violater Indices (SAVI),
- Border Crossing Information System (BCIS),
- Department of State visa databases,
- TECS seizure data, and
- terrorist watchlists that are subsets of the U.S. government's Terrorist Screening Database.[47]

In DHS's ATS Privacy Impact Assessment, the department underscored that ATS-Passenger uses the same methodology for all individuals, a practice that arguably precludes the possibility of disparate treatment of individuals or groups.[48] ATS-Passenger, moreover, does not assign a score to determine an individual's risk. Rather, it compares PNR data for all travelers against the systems/databases listed above to identify matches with law enforcement lookouts as well as patterns of suspicious activity that have been discerned through past investigations and intelligence.[49]

In conclusion, ATS-Passenger enables DHS to distinguish those passengers who may pose a risk earlier and in ways that would be impossible during primary inspection at a port of entry.[50] DHS claims that these efforts have had measurable success, resulting in the identification of known and

---

[44] U.S. Department of Homeland Security, *Statement By Homeland Security Secretary Michael Chertoff On A New Agreement With The European Union for Passenger Name Record Data Sharing*, July 26, 2007.

[45] Ibid.

[46] Ibid.

[47] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System*, August 3, 2007, p. 5.

[48] Ibid, p. 4.

[49] Ibid, p. 5.

[50] CBP briefing provided to CRS on November 14, 2008.

suspected terrorists in addition to other criminals such as narcotics smugglers, travelers with fraudulent documents, and lost/stolen passports, all of whom would have otherwise gone undetected.[51] As described below, the FAA also developed a similar decision support tool in the mid-1990s known as CAPPS, which has been inherited by TSA.

TSA "No Fly" and "Automatic Selectee" Watchlists

The TSA provides the airlines with the "No Fly" and "Automatic Selectee" watchlists for use in identifying passengers who are to be denied boarding or who require additional scrutiny prior to boarding. The "No Fly" watchlist is a list of persons who are considered a direct threat to U.S. civil aviation. Aircraft bombings in the late 1980s prompted the U.S. government to adopt this list in 1990. It was initially administered jointly by the FBI and Federal Aviation Administration (FAA), but the FAA assumed sole administrative responsibility for this list in November 2001. At that time, the FAA instituted the "Automatic Selectee" list as well. As the names of these lists imply, prospective passengers found to be on the "No Fly" list are denied boarding and referred to law enforcement, whereas those on the "Automatic Selectee" list are selected for secondary security screening before being cleared to board.

Under the Aviation Transportation Security Act,[52] TSA was established and assumed the administrative responsibility for these lists. As the FAA did before it, the TSA distributes these watchlists to U.S. air carriers. In turn, the air carriers screen passengers against these watchlists before boarding. In general, these lists are downloaded into a handful of computer reservations systems used by most U.S. air carriers; however, a few smaller carriers still manually compare passenger data against these lists. As intelligence and law enforcement officials were concerned about the security of the "No Fly" list, only a handful of names were listed prior to the 9/11 attacks (fewer than 20).[53] Since then, the lists have been expanded almost daily.[54] Within TSA, the Office of Intelligence is responsible for resolving potential watchlist matches.

According to the FBI, the "No Fly" and "Automatic Selectee" lists were consolidated into the TSC's TSDB sometime in the latter half of FY2004.[55] While much larger, these watchlists still appear to be a relatively small subset of the TSDB. It has been reported that by the end of FY2004, there were more than 20,000 names on the "No Fly" list and TSA was being contacted by air carriers as often as 30 times per day with potential name matches.[56] During 2004, the "No Fly" and "Automatic Selectee" lists were the subject of increased media scrutiny for

---

[51] Ibid.

[52] Public 107-71, Nov. 19, 2001, 115 Stat. 597.

[53] National Commission on Terrorist Attacks Upon the United States, *The Aviation Security System and the 9/11 Attacks*, Staff Statement no. 3, January 27, 2004, p. 6.

[54] Electronic Privacy Information Center, "'Documents Show Errors in TSA's 'No Fly' Watchlist," April 2003, at http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.

[55] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, "Terrorist Screening Center Consolidates Data for Law Enforcement Needs," *The CJIS LINK*, vol. 7, no. 4, October 2004, pp. 1-2.

[56] Sara Kehaulani Goo, "Faulty 'No Fly' System Detailed," *Washington Post*, October 9, 2004, p. A01.

misidentifications. In some cases, these misidentifications included Members of Congress (e.g., Senator Edward Kennedy and Representatives John Lewis and Don Young).[57]

It is notable that because not all known and suspected terrorists are considered "threats to civil aviation," there could be legal and investigative policy considerations that would bear upon placing all such persons, who are included in the TSDB, on the "No Fly" list and possibly the "Automatic Selectee" list. The TSC, moreover, may be reluctant to release the full list of known and suspected terrorists to the airlines because of data security concerns. Although data security remains a concern, a much larger terrorist watchlist is provided by the TSC to CBP. This watchlist, however, remains under government control.

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) included two reporting requirements related to air passenger prescreening and terrorist watchlists. Section 4012(b) required the DHS Privacy Officer to report to Congress,[58] within 180 days of enactment (June 15, 2005), on the impact of the "No Fly" and "Automatic Selectee" lists on privacy and civil liberties. Section 4012(c) required the National Intelligence Director, in consultation with the Secretary of Homeland Security, the Secretary of State, and the Attorney General, to report to Congress, within a 180 days of enactment, on the criteria for placing individuals in the consolidated TSDB watchlists maintained by the TSC, including minimum standards for reliability and accuracy of identifying information, the threat levels posed by listed persons, and the appropriate responses to be taken if those persons were encountered.

In April 2006, the DHS Privacy Office issued its report assessing the impact of the "No Fly" and "Automatic Selectee" lists on privacy and civil liberties.[59] The report cited concerns about the quality of the information of those lists, as well as the underlying intelligence.[60] The report also noted allegations about profiling on the basis of race, religion, or national origin, but reported that it could not substantiate those allegations.[61] Furthermore, the report assessed existing DHS redress mechanisms, which are described briefly below.

In regard to the criteria used to place individuals on terrorist watchlists consolidated in the TSDB, it is unknown whether the National Intelligence Director reported to Congress on this matter. Nevertheless, the Privacy Office report stressed that those criteria could not be made public without (1) compromising intelligence and security or (2) allowing persons wishing to avoid

---

[57] Sara Kehaulani Goo, "Committee Chairman Runs Into Watch-List Problem: Name Similarity Led to Questioning at Anchorage and Seattle Airports, Alaska Congressman Says," *Washington Post*, Sept. 30, 2004, p. A17; and "Hundreds Report Watch-List Trials: Some Ended Hassles at Airports by Making Slight Change to Name," *Washington Post*, August 21, 2004, p. A08.

[58] Section 4012(b) of P.L. 108-458 required that the report be submitted to the Committee on the Judiciary, the Committee on Governmental Affairs and Homeland Security, and the Committee on Commerce, Science, and Transportation in the Senate; and to the Committee on the Judiciary, the Committee on Government Reform, the Committee on Transportation and Infrastructure, and the Committee on Homeland Security in the House of Representatives.

[59] U.S. Department of Homeland Security, *DHS Privacy Office Report on Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties*, April 27, 2006, 22 pp.

[60] Ibid., p. 8.

[61] Ibid., p. 9.

detection to subvert those lists.[62] In October 2007, the GAO reported that the FBI and Intelligence Community were using reasonable standards for watchlisting persons who are suspected of having possible links to terrorism.[63]

On January 17, 2007, the head of TSA, Assistant Secretary Edmund "Kip" Hawley, testified before the Senate Committee on Commerce, Science and Transportation about aviation security and related recommendations made by the National Commission on Terrorist Attacks upon the United States (9/11 Commission).[64] With regard to terrorist watchlist screening of air passengers, Assistant Secretary Hawley informed the committee that TSA and the Terrorist Screening Center were reviewing the "No Fly" list in an effort to reduce the number of individuals on that list by as much as 50%.[65] According to a press account, the "No Fly" list includes 4,000 names of individual persons and the "Selectee" lists includes about 14,000 names.[66]

Computer-Assisted Passenger Prescreening System (CAPPS)

The 1996 Federal Aviation Reauthorization Act authorized the development of the Computer-Assisted Aviation Prescreening System (CAPS) system.[67] At the time this bill was enacted, however, the Federal Aviation Administration (FAA) had already begun to develop the system that became CAPS.[68] The FAA, together with Northwest Airlines, developed the CAPS interface with the airline's computer reservation system in 1996 and 1997. Additional field testing continued through 1997 and 1998. The FAA issued a proposed rule directing all major U.S. air carriers to maintain CAPS on their computer reservation systems in April 1999.[69] However, this rule was never made final, reflecting in part the controversy generated by this system.

---

[62] Ibid.

[63] U.S. Government Accountability Office, *Terrorist Watch List Screening, Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand the Use of the List*, GAO-08-110, October 2007, p. 19.

[64] U.S. Department of Homeland Security, Testimony of Assistant Secretary Edmund S. Hawley before the Senate Committee on Commerce, Science and Transportation, "Aviation Security and 9/11 Commission Recommendations," January 17, 2007.

[65] Ibid.

[66] Carrie Johnson, "Explosive Could Have Blown Hole in Plane: President Orders Review of Watch Lists as Criticism Intensifies," *Washington Post*, December 29, 2009, p. A4.

[67] P.L. 104-264; 110 Stat. 3253. Section 307 of the act reads: "The Administrator of the Federal Aviation Administration, the Secretary of Transportation, the intelligence community, and the law enforcement community should continue to assist air carriers in developing computer-assisted passenger profiling programs and other appropriate passenger profiling programs which should be used in conjunction with other security measures and technologies."

[68] Also, during this time, the White House Commission on Aviation Safety and Security (Gore Commission) recommended that an automated profiling system for commercial aviation be developed. See *White House Commission on Aviation Safety and Security: Final Report to President Clinton*, February 12, 1997.

[69] 64 *Federal Register*, pp. 19219-19240, April 19, 1999.

CAPS and Checked Baggage Screening

The operational concept behind the CAPS system is to select "high-risk" travelers based on certain characteristics found in *passenger name record* (PNR) data elements—like ticket purchasing patterns and the details of their travel itineraries for greater scrutiny in terms of baggage screening, while expediting baggage screening for "low-risk"passengers. In other words, the CAPS system was designed to determine which passengers were unlikely to have an explosive device in their checked baggage, so that limited explosive detection capabilities could be focused on a smaller number of passengers and bags.[70] The CAPS system was reviewed by the Department of Justice's Civil Rights and Criminal Divisions, along with the FBI, and was found not to be based on characteristics related to ethnicity, gender, or religious faith.[71] The CAPS system was later renamed CAPPS (Computer-Assisted Passenger Presceening System). Like the "No Fly" and "Automatic Selectee" watchlists, the CAPPS system is largely invisible to the public as the system itself resides on airline reservations systems (for example, Sabre and Amadeus).[72] The federal government, moreover, does not control or collect data utilized by CAPPS.

CAPPS and Passenger Screening at Airport Security Checkpoints

It is significant to note that, on September 11, 2001, nine of the 19 hijackers were selected by CAPPS for additional *baggage* screening; however, CAPPS was not used to select *passengers* for greater screening at passenger checkpoints.[73] Since the 9/11 attacks, CAPPS has been expanded, and TSA uses the system to identify persons based on certain characteristics gleaned from the PNR data who are selected for not only additional passenger-checked baggage screening, but additional passenger checkpoint screening as well.

9/11 Commission Recommendations and CAPPS II

The 9/11 Commission formally recommended that the "no fly" and "automatic selectee" lists should be improved, and that air passengers should be screened not only against these lists, but the "larger set of watchlists maintained by the federal government."[74] Moreover, the TSA should perform this function, as opposed to the air carriers, and the air carriers should be required to supply the information needed to test a new air passenger prescreening system.[75]

---

[70] Statement of Jane Garvey to the National Commission on Terrorist Attacks Upon the United States, May 22, 2003, p. 11.

[71] Anthony Fainberg, "Aviation Security in the United States: Current and Future Trends," Transportation Law Journal, vol 25, spring 1998, p. 200.

[72] Ibid., p. 200.

[73] Statement of Cathal L. Flynn to the National Commission on Terrorist Attacks Upon the United States, January 27, 2004, p. 4.

[74] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, Authorized ed. (New York: W.W Norton & Co., 2004), p. 393.

[75] Ibid.

When the 9/11 Commission report was released in July 2004, the TSA had already been working for almost two years on a new passenger prescreening system called CAPPS II. This system was intended to replace the airline-operated systems for checking passenger names against the government-issued "no-fly" watchlist (those individuals to be denied boarding) and the "automatic selectee" watchlist (those individuals designated for additional or secondary screening at airport security checkpoints). In addition, in lieu of a biometric, CAPPS II was designed to include sophisticated algorithms that would query both government and commercial databases to authenticate the identity of passengers and crew, as well as assess their risk.

Critics argued, however, that the TSA's ever-expanding vision for prescreening constituted an unprecedented government-sponsored invasion of privacy. This and other controversies ultimately led TSA to scrap CAPPS II in August 2004, soon after the release of the 9/11 Commission final report, and pursue enhanced prescreening capabilities under a new system called Secure Flight. As described below, TSA planned to begin implementing Secure Flight in December 2008, but actual implementation did not begin until March 2009. Although, the original scope of the Secure Flight has also been scaled back so that it no longer includes an identity authentication component or a rule for more intensive searching, TSA has not announced any plans to discontinue the use of CAPPS.

TSA Secure Flight Program

Reflecting the recommendations of the 9/11 Commission, Congress included several provisions related to preflight screening of airline passengers against terrorist watchlists in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). In particular, section 4012 of that act requires the TSA to assume from U.S. air carriers the passenger watchlist screening function after it establishes an advanced (pre-departure) air passenger prescreening system that utilizes the greater set of watchlists integrated and consolidated in the FBI-administered Terrorist Screening Database (TSDB). It also required the DHS to screen passengers on international flights against the TSDB prior to departure, a requirement currently met by CBP through its APIS pre-departure process (described above). Following the demise of CAPPS II (described above), TSA has sought to address the mandate for domestic passenger prescreening though the development of the Secure Flight system and plans to eventually incorporate international passenger prescreening under this system as well, following its successful implementation domestically.

Initial Program Design, Development, and Related Legislation

As initially conceived by TSA, the Secure Flight program was designed to improve passenger prescreening and deter, detect, and prevent known or suspected terrorists from boarding commercial flights. The TSA endeavored to meet this objective by using Secure Flight as a means to focus its limited screening resources on individuals and their baggage who are perceived to pose an elevated or unknown risk to commercial aviation, while reducing the number of passengers screened and wait times at passenger screening checkpoints. According to TSA, Secure Flight consisted of four elements:

- a streamlined rule for more intensive screening,
- a scaled-back identity authentication process,
- a passenger name check against the Terrorist Screening Database, and

- an appeals process for passengers who may have been misidentified.

In addition to the appeals process, the Secure Flight program is an amalgam of features taken from existing screening systems, CAPPS II, and the 9/11 Commission's recommendations that passengers be screened against the wider set of terrorist watchlists maintained by the U.S. government. Within TSA, the Office of National Risk Assessment had responsibility for establishing policy for the Secure Flight program.

To reduce redundant or overlapping passenger processing systems, TSA initially planned to design Secure Flight so that the system would be used *only* for prescreening passengers on *domestic* flights. As described above, DHS's CBP would continue to be responsible for checking passenger identities against watchlists and prescreening passengers on inbound and outbound *international* flights. It was unclear, however, whether responsibility for screening domestic and international flights could clearly be divided between TSA and CBP, because many international flights have domestic legs and international passengers sometimes make connections to domestic flights.

It was also unclear, moreover, whether the development of Secure Flight for domestic flight would impair TSA's responsibility for screening international air passengers who may be threats to civil aviation. At issue is TSA's authority and responsibility over all aspects of aviation security versus CBP's authority and responsibility for border management and security. It remained an open policy question whether the CBP pre-departure screening of air passengers on all in-bound international flights through APIS would be sufficient. In the case of international air travel, the distinction between aviation and border security functions has become increasingly blurred.

Problems Developing Secure Flight

Like its predecessor, CAPPS II, the Secure Flight program initially proved controversial. In March 2005, the DHS OIG reported that TSA had mishandled some passenger data while testing CAPPS II, but since that time, the agency's approach to privacy issues had improved markedly.[76] In the same month, the GAO reported that TSA had begun developing and testing Secure Flight; however, TSA had not determined fully "data needs and system functions," despite ambitious timelines for program implementation.[77] Consequently, the GAO reported that it was uncertain whether TSA would meet its August 2005 Secure Flight operational deployment date.[78] The TSA, in fact, did not meet the deadline and in February 2006 announced that it was restructuring ("rebaselining") the Secure Flight program.

In addition, in July 2005, GAO reported that TSA had not fully disclosed its use of passenger data during the testing for Secure Flight.[79] In August 2005, the DOJ OIG reported that there were

---

[76] U.S. Department of Homeland Security, Office of Inspector General, *Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data (Redacted)*, OIG-05-12, March 2005, p. 8.

[77] U.S. Government Accountability Office, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*, GAO-05-356, March 28, 2005, p. 17.

[78] Ibid.

[79] U.S. Government Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully* (continued...)

numerous problems coordinating the development of the Secure Flight program with the efforts of the FBI-administered TSC.[80] In September 2005, the identity authentication element of the Secure Flight program, under which TSA planned to compare PNR data (for domestic flights) with databases maintained by commercial data aggregators to verify passenger identities, was reportedly dropped.[81] In December 2006, moreover, the DHS's Privacy Office issued a report, finding that the TSA had not accurately described its use of personal data as part of the Secure Flight program in notifications required under the Privacy Act.[82]

Furthermore, in the FY2005 DHS Appropriations Act (P.L. 108-334), Congress prohibited TSA (or any other component of DHS) from spending any appropriated funds on the deployment of Secure Flight, or any successor system used to screen aviation passengers, until the GAO reports that certain conditions have been met, including the establishment of an appeals process.[83] Similar provisions have been included in subsequent departmental appropriations, including the FY2009 DHS Appropriations Act (P.L. 111-5).[84] As noted above, TSA began implementing Secure Flight domestically in March 2009. In the FY2010 DHS Appropriations Act (P.L. 111-83), Congress did not include a similar spending prohibition; however, report language requires TSA to report within 90 days on its progress in addressing GAO's Secure Flight-related recommendations.

Secure Flight Final Rule

On October 28, 2008, TSA published a final rule detailing the operational implementation of Secure Flight, effective December 29, 2008.[85] TSA is implementing Secure Flight in two phases. The first phase encompasses only *domestic* flights, while the second phase will include *international* departures and arrivals as well as commercial international flights overflying any of the 48 contiguous states. TSA began operational testing in May 2009 to test the reliability of data transmission connections to receive passenger data from the airlines and transmit screening results back to the airlines, and to assess the performance of the watch list screening process under operational conditions. Operational testing and phased-in implementation of Secure Flight for vetting domestic passengers is currently underway. Effective August 15, 2009, airlines were required to begin collecting full name, date of birth, gender, and redress number (if available) for domestic passengers. The airlines were required to begin collecting such information for international passengers effective October 31, 2009. The TSA has stated that its goal is to fully

(...continued)

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, July 22, 2005, p. 9.

[80] U.S. Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, Audit Report 05-34, August 2005, 41 pp.

[81] John Bacon, "TSA: 'Data Mining' Deleted from Plan," *USA Today*, September 23, 2005, p. 3A.

[82] U.S. Department of Homeland Security, Privacy Office, *Secure Flight Report: DHS Privacy Office Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations*, December 2006, 15 pp.

[83] Sec. 522, 118 Stat. 1319.

[84] Sec. 513, 121 Stat. 2072.

[85]U.S. Department of Homeland Security, Transportation Security Administration, "Secure Flight Program; Final Rule," 72 *Federal Register*, pp. 64018-64066, October 28, 2008.

implement Secure Flight for domestic flights by early 2010, and for all international flights by the end of 2010.[86]

During the time operational testing of Secure Flight is ongoing, airlines will be required to continue the process of checking passengers against the "no fly" and "automatic selectee" lists provided by TSA. As a result, TSA will continue to distribute these lists to airlines until all airlines have completed operational testing of the domestic portion of Secure Flight and TSA assumes full responsibility for comparing passenger data against the terrorist watch list.

For international flights, CBP will continue to check passenger names against terrorist watch lists under the APIS pre-departure protocols until Secure Flight in fully implemented for international flights. However, airlines will transmit data using a single transmission DHS portal, although the two systems have slightly different data requirements and different timetables for the delivery of data, as explained in the Secure Flight final rule.

Overflights[87] represent a new category of covered operations that will require transmission of passenger data for screening against the terrorist watch list and will encompass operators that may not operate flights to and from the United States. According to the final rule, the phase in of overflights in the Secure Flight system will coincide with the phase in of international flights.

Secure Flight and Terrorist Watchlist Checks

Initially, the TSA will begin implementing the use of Secure Flight to compare passenger data (Secure Flight Passenger Data) provided by the airlines against the TSDB. This will replace the process of providing these "automatic selectee" and "no fly" lists to the airlines. The program will apply to passenger airlines offering scheduled passenger service and public charter flights that operate to and from about 450 commercial passenger airports throughout the United States. These airlines will be required to submit passenger data to the TSA beginning 72 hours prior to the flight and thereafter continue to provide passenger data as soon as it becomes available. The airlines must also submit this required information for any non-employee seeking access to the sterile area beyond the security screening checkpoint, such as an individual assisting a special needs traveler or escorting an unaccompanied minor to or from an aircraft. The airlines will be required to collect from all passengers and individuals seeking access to the airport sterile area their full name, date of birth, and gender data. The airline must also request from travelers any known traveler[88] or passenger redress number provided by the TSA and, if these numbers are provided by the passengers, then the airline must transmit them to the TSA. The airline must also

[86] Transportation Security Administration, "TSA's Secure Flight Enters First Public Phase," May 12, 2009.

[87] Overflights refer to flights that transit through the airspace above a geographic area but do not originate or land at a destination in that area. As noted previously, Secure Flight requirements will only be applied to those overflights transiting through airspace over the contiguous 48 states and will not include aircraft overflying Alaska or Hawaii.

[88] The TSA Secure Flight final rule explains that this Known Traveler Number would be a unique number assigned to a traveler for whom the federal government has already conducted a threat assessment and was found to not pose a security threat. Since the TSA eliminated the requirement for security threat assessments for passengers participating in the voluntary Registered Traveler (RT) program effective July 30, 2008, it does not appear that the Known Traveler Number field will be propagated with RT number data at this point, and it is not believed that RT participation will, at present, have any impact on the name based threat assessment process to be conducted under the Secure Flight program.

transmit passport numbers, itinerary information, record locator data, and various other reference numbers if these data are available. For a complete list of Secure Flight Passenger Data (SFPD), see **Appendix D**.

Once received, the TSA will use an automated process to compare this passenger data against the consolidated TSDB. The TSA does not maintain its own watch list, but rather the TSA is a customer of the TSC. In consultation with the TSA, the TSC compiles the "no fly" and "automatic selectee" lists from the consolidated TSDB. Under the Secure Flight system, TSA will similarly continue to rely on the TSDB to determine whether to deny a passenger boarding or subject the passenger and his or her property to additional physical screening.

When the Secure Flight process returns an indication of an exact or reasonably similar match, a TSA intelligence analyst will review additional available information in an effort to reduce the number of false positive matches. If the TSA determines that a probable match exists, it will forward these results along with the passenger information to the TSC to provide confirmation of the match. According to the procedures set forth in the Secure Flight final rule, if the TSA or the TSC cannot make a definitive determination, notification would be sent to the airline to require the passenger to present a verifying identity document (VID), such as an unexpired driver's license or a passport, when checking in at the airport. If the TSA determines that the passenger data provided is a match to the Secure Flight selectee list, it will inform the airline which, in turn, will be required to identify the passenger and his or her baggage for enhanced screening. The TSA may also inform an airline that a passenger is to be placed in "inhibited status," meaning that he or she may not be issued a boarding pass or enter the sterile area of an airport.

Passengers who believe that they have been wrongly delayed, denied boarding, or subject to additional screening as a result of the Secure Flight system and the process it applies to screening passenger data against terrorist watch list information may seek redress from the DHS. The procedures for redress apply to all DHS-operated systems for screening individuals against terrorist watch list data and are described in further detail below.

Misidentifications and Related Procedures

Misidentifications have been a recurring issue for Congress. Initially, such problems were frequently associated with TSA's administration of the "No Fly" and "Automatic Selectee" lists. More recently, however, this may be an emerging problem for CBP as well in light of the American Civil Liberties Union (ACLU) class-action suit against that agency.[89]

Under HSPD-6, the TSC Director has been made responsible for developing policies and procedures related to the criteria for including terrorist identities data in the consolidated TSDB and for measures to be taken in regard to misidentifications, erroneous entries, outdated data, and privacy concerns. The Bush Administration maintained further that because the TSC does not

[89] According to the ACLU, U.S. citizens have been subjected to repeated and lengthy stops, questioning, body searches, handcuffing, excessive force, and separation from family while being detained by CBP officers because of possible watchlist matches. Nine of these U.S. citizens have filed a class action suit against DHS. See *Rahman v. Chertoff*, Case No. 05 C 3761 (E.D. Ill. filed June 19, 2006).

collect intelligence, and has no authority to do so, all intelligence or data entered into the TSDB are actually being collected by other agencies in accordance with applicable, pre-existing authorities.

At the same time, however, the TSC is limited in its ability to address certain issues related to misidentifications because it is restricted from divulging classified or law enforcement-sensitive information to the public under certain circumstances (discussed below). The same could be said for many frontline-screening agencies as well (e.g., TSA and CBP), because many terrorist lookout records, while possibly declassified, are based on classified intelligence collected by other agencies. Such records would probably be considered security sensitive information. Hence, questions could arise as to which agencies, if any, are in a position to handle matters pertaining to misidentifications.

Moreover, if procedures are not properly coordinated, inconvenienced travelers who have been misidentified as terrorists or their supporters could face a bureaucratic maze if they attempt to seek redress and remedy. The DOJ OIG audit on TSC operations (described above) included a recommendation that the TSC strengthen procedures for handling misidentifications and articulate those procedures formally in written documents (operational guidelines).[90] Congress later required reports from the Administration and GAO regarding the use of terrorist watchlists.

Disclosure Under FOIA and Privacy Act

In regard to TSC, Members of Congress and other outside observers have questioned whether there should be new policy and procedures at different levels (such as visa issuance, border inspections, commercial aviation security, domestic law enforcement, and security of public events) for the inclusion of persons in the TSDB.[91] Also, Members have asked how a person could find out if they were in the Terrorist Screening Database and, if so, how they got there. In congressional testimony, then-TSC Director Bucella surmised that a person would learn of being in the TSDB when a screening agency encountered them and, perhaps, denied them a visa or entry into the United States, or arrested them. Bucella suggested that the TSC would probably be unable to confirm or deny whether the person was in the TSDB under current law.[92]

Consequently, persons who have been identified or misidentified as terrorists or their supporters would have to pursue such matters through the screening agency. The screening agency, however, might not have been the originating source of the record, in which case a lengthy process of referrals may have to be initiated. Under such conditions, persons identified as terrorists or their supporters may turn to the Freedom of Information Act (FOIA) or the Privacy Act as a last alternative. Under FOIA,[93] any person, including a noncitizen or nonpermanent resident, may file a request with any executive branch agency or department, such as the State Department or DHS,

---

[90] Ibid., p. 76.

[91] For further information, see CRS Report RL31730, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws*, by Gina Stevens.

[92] Donna Bucella, Terrorist Screening Center Director, Testimony Before the National Commission on Terrorist Attacks upon the United States, January 26, 2004, p. 1.

[93] 5 U.S.C. §522.

for records indicating he or she is on a watchlist. However, under national security and law enforcement FOIA exemptions, the departments may withhold records on whether an individual is on a watchlist.[94] Consequently, a FOIA inquiry is unlikely to shed any light on these areas.

In addition, a citizen or legal permanent resident may file a Privacy Act[95] request with DHS and/or DOJ to discern whether a screening agency or the FBI has records on them. However, the law enforcement exemption under the Privacy Act may permit the departments to withhold such records. Under the Privacy Act, a citizen or legal permanent resident may request an amendment of their record if information in the record is inaccurate, untimely, irrelevant, or incomplete. Under both FOIA and the Privacy Act, there are provisions for administrative and judicial appeal. If a request is denied, the citizen or legal permanent resident is required to exhaust his or her administrative remedies prior to bringing an action in U.S. District Court to challenge the agency's action.[96]

Other Possible Legal Questions

The Bush Administration pledged that terrorist screening information would be gathered and employed within constitutional and other legal parameters. CRS is unaware of any official statement by the Obama Administration regarding these matters. Nevertheless, although the Privacy Act generally does not restrict information sharing related to known and suspected terrorists who are not U.S. persons for the purposes of visa issuance and border inspections, it does restrict the sharing of information on U.S. persons (citizens and legal permanent residents) for purely intelligence purposes, who *are not* the subject of ongoing foreign intelligence or criminal investigations.[97] Consequently, legal questions concerning the inclusion of U.S. persons on various watchlists under criminal or national security predicates may arise. In addition, questions of compensation for persons damaged by mistaken inclusion in these databases will likely be an issue.

DHS Redress Mechanisms

Both the DHS Privacy Office and GAO reported to Congress on existing DHS redress mechanisms, by which an individual who felt he or she had been unfairly denied boarding on a commercial aircraft or singled out for screening could contact several DHS offices and initiate a redress inquiry.

---

[94] 5 U.S.C. §§522(b), (c), 522a(j).

[95] 5 U.S.C. §522a.

[96] One recent legal analysis examined several U.S. court decisions addressing the use of terrorist watchlists for aviation security purposes. According to that analysis, it appears that the presiding judges in those cases were willing to defer to TSA regarding determinations that watchlist records were security sensitive information, even though those records were essential to the maintenance of the plaintiffs' claims. See Linda L. Lane, "The Discoverability of Sensitive Security Information in Aviation Litigation," *Journal of Air Law and Commerce*, vol. 71, Summer 2006, p. 434

[97] Department of State, *Testimony to the Joint Congressional Intelligence Committee*, p. 5.

Early Mechanisms

According to the DHS Privacy Office, individuals who believed they had been misidentified as a terrorist while being screened by TSA could have contacted either the TSA Ombudsman's Contact Center or Office of Civil Rights.[98] Information was also available on the TSA website regarding the redress process.[99] Individuals seeking redress were issued a Privacy Act Notice and Passenger Identity Verification Form, which was processed by the TSA Office for Transportation Security Redress (OSTR).[100] If OSTR concluded an individual had been misidentified, it would place him or her on a "cleared" list.[101] However, GAO reported that individuals who had been placed on the cleared lists could have continued to encounter inconveniences. For example, "they may be forced to obtain a boarding pass at the ticket counter as opposed to the using the Internet, curbside, or airport kiosk check-in options."[102]

Meanwhile, individuals who believe they have been misidentified while being screened by CBP could contact that agency's Customer Service Satisfaction Unit.[103] In addition to contacting either TSA or CBP, individuals who had possibly been misidentified could have also contacted either the DHS Privacy Office or Office of Civil Rights and Civil Liberties.[104] As described above, frontline-screening agencies referred matters concerning individuals who believe they have been mistakenly watchlisted to the TSC, as is the case today.

At a Senate hearing, the former head of TSA, Assistant Secretary Hawley, conceded that the redress processes at TSA had been "too cumbersome and expensive," prompting the agency to introduce a new streamlined process and automated redress management system.[105] Hawley also testified that then-DHS Secretary Chertoff had developed a program envisioned by then-Secretary of State Condoleezza Rice that is designed to provide travelers with a single, simple process for addressing watchlist-related complaints.[106] Hawley also testified that the advance air passenger prescreening program known as Secure Flight would reduce misidentifications—the largest source of complaints.[107] He reported that TSA had processed more than 20,000 redress requests in 2006, and the average processing times of those requests had been reduced from two months to 10 days.[108]

---

[98] U.S. Department of Homeland Security, *DHS Privacy Office Report on Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties*, April 27, 2006, p. 17.

[99] Ibid.

[100] Ibid.

[101] Ibid.

[102] U.S. Government Accountability Office, *Terrorist Watch List Screening*, GAO-06-1031, Sept. 2006, p. 34.

[103] U.S. Department of Homeland Security, *DHS Privacy Office Report on Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties*, April 27, 2006, p. 17.

[104] Ibid.

[105] U.S. Department of Homeland Security, Testimony of Assistant Secretary Edmund S. Hawley before the Senate Committee on Commerce, Science and Transportation, "Aviation Security and 9/11 Commission Recommendations," January 17, 2007.

[106] Ibid.

[107] Ibid.

[108] Ibid.

Traveler Redress and Inquiry Program (TRIP)

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required the TSA and DHS to establish appeals procedures by which persons who are identified as security threats based on records in the TSDB may appeal such determinations and have such records, if warranted, modified to alleviate such occurrences in the future. Also, provisions in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) required the DHS to establish an Office of Appeals and Redress to establish a timely and fair process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. The provisions further establish a requirement to maintain records of those passengers and individuals who have been misidentified and have corrected erroneous information.

To handle and resolve the complaints of passengers and meet these statutory requirements, the DHS has established the DHS Traveler Redress Inquiry Program (DHS TRIP) as a mechanism for addressing watchlist misidentification issues and other situations where passengers feel that they have been unfairly or incorrectly delayed or denied boarding or identified for additional security screening at airport screening checkpoints, ports of entry or border checkpoints, or when seeking to access other modes of transportation.

The DHS TRIP program allows passengers seeking redress, or their lawyers or other representatives, to file complaints either by using an online system or by completing and mailing a complaint form.[109] After completing the online questionnaire or mailing the complaint form, the DHS will request supporting information within 30 days. Filers are given a control number that allows them to track the status of their inquiry using the Internet. The DHS will make a final determination and respond to the filer. If the investigation finds that the traveler has been delayed due to a misidentification or similar name-matching issue, the response will describe the steps required to resolve this issue. Often, the traveler may be required to retain a copy of the DHS response letter and present it during the check-in process when traveling on airline flights. The DHS cautions, however, that the steps taken may not resolve all future travel-related concerns. For example, the traveler may be selected for additional screening based on a variety of factors or at random. If a passenger disagrees with the resolution decision made by the DHS, he or she may take further steps to appeal the decision.

Fair, Accurate, Secure, and Timely (FAST) Redress Act of 2009 (H.R. 559)

In the 111th Congress, the House passed the FAST Redress Act (H.R. 559) under suspension of the rules on February 3, 2009, a bill introduced by Representative Yvette D. Clarke. This bill is similar to a proposal (H.R. 4179) passed in the 110th Congress, also introduced by Representative Clarke. The House Committee on the Judiciary reported H.R. 4179 (H.Rept. 110-686) on June 5,

[109] Complete instructions for filing complaints under the DHS TRIP program can be found at: http://www.dhs.gov/files/programs/gc_1169676919316.shtm.

2008. The House passed H.R. 4179 on June 18, 2008. Senator Amy Klobuchar introduced an identical proposal (S. 3392). The FAST Redress Act would amend the Homeland Security Act of 2002 (P.L. 107-296) to direct the Secretary of Homeland Security to establish a timely and fair process for individuals who believe they were delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat when screened against any terrorist watchlist or database used by TSA or any component of DHS. It would also authorize an Office of Appeals and Redress within DHS to implement, coordinate, and execute this process.

Possible Issues for Congress

Three issues loom large in terms of the U.S. government's capabilities to identify, screen, and track terrorists and their supporters. For example, how reliable is the intelligence that is the basis for lookout records? When will the TSA and CBP be able to prescreen effectively air passengers *prior to departure*? Will the TSC in cooperation with screening agencies be able to establish viable redress and remedy processes for persons misidentified as terrorists or their supporters given certain limitations placed on those agencies in regard to the public divulgence of national security and law enforcement sensitive information?

Reliability of Intelligence Underlying Lookout Records

Because the Terrorist Identities Datamart Environment (TIDE) maintained by the National Counterterrorism Center (NCTC) is the principal source of lookout records on international terrorists placed in the TSC's consolidated terrorist screening database, a key oversight issue for Congress is ensuring that intelligence community agencies are sharing the appropriate information necessary to identify terrorists and their supporters with the NCTC. Is the TSC receiving timely terrorist identities data updates that reflect the best and most reliable intelligence available to intelligence and law enforcement agencies?

Preflight Passenger Screening by TSA and CBP

While largely related to implementation, a number of unresolved questions remain with regard to prescreening air passengers prior to departure (wheels up). How quickly can TSA develop and deploy an advanced air passenger prescreening system that, among other things, will assume the day-to-day administration of the "No Fly" and "Automatic Selectee" watchlists from the airlines?

Viable Processes of Redress and Remedy for Misidentifications

Concerning misidentifications, under HSPD-6, the TSC Director is responsible for developing policies and procedures related to the criteria for inclusion into the consolidated TSDB, and for taking measures to address misidentifications, erroneous entries, outdated data, and privacy concerns. An issue for Congress may be the extent to which the TSC is working with screening agencies to develop appropriate and effective redress and remedy processes for persons misidentified as terrorists or their supporters. Given certain limitations placed on the TSC and screening agencies with regard to releasing national security and law enforcement sensitive information, will sufficient information channels be available and remedial processes established to provide for accurate and expeditious determinations in misidentification cases?

Appendix A. APIS Data Elements

APIS data elements include the following:

- Full Name.
- Date of Birth.
- Gender.
- Passport Number.
- Passport Country of Issuance.
- Passport Expiration Date.
- Passenger Name Record Locator.
- Foreign Airport Code—place of origination.
- Port of First Arrival.
- Final Foreign Port for In-transit Passengers.
- Airline Carrier Code.
- Flight Number.
- Date of Aircraft Departure.
- Time of Aircraft Departure.
- Date of Aircraft Arrival.
- Scheduled time of Aircraft Arrival.
- Citizenship.
- Country of Residence.
- Status on Board Aircraft.
- Travel Document Type.
- Alien Registration Number.
- Address in the United States (except for outbound flights, U.S. citizens, lawful permanent residents, and crew and in-transit passengers).[110]

[110] 73 *Federal Register*, pp. 64023-64024, October 28, 2008.

Appendix B. PNR Data Elements

PNR data elements include the following:

- PNR record locator code.
- Date of reservation/issue of ticket.
- Date(s) on intended travel.
- Name(s).
- Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.).
- Other names on PNR, including number of travelers on PNR.
- All available contact information (including originator of reservation).
- All available payment/bill information.
- Travel itinerary for specific PNR.
- Travel agency/travel agent.
- Code share information.
- Split/divided information.
- Travel status of passenger (including confirmations and check-in status) and relevant travel history.
- Ticketing information, including ticket number, one way tickets, and Automated Fare Quote (ATFQ) fields.
- Baggage information.
- Seat information.
- Open text fields.
- Any collected APIS information.
- All historical changes to the PNR listed above.[111]

[111] U.S. Department of Homeland Security, "Letter from the United States to the Council of the European Union," July 26, 2007, p. 2.

Appendix C. EU-U.S. Data Sharing

In Summer 2006, the issue of PNR data sharing emerged as a problem for the United States. Although the European Court of Justice had ruled an EU-U.S. PNR data sharing agreement to be illegal and ordered a cessation of such data sharing on September 30, 2006, then-DHS Secretary Chertoff proposed that the United States should acquire greater amounts of PNR data to improve passenger prescreening for known and suspected terrorists following the foiled plot to bomb airliners flying from the UK to the United States in August 2006.[112] An interim EU-U.S. agreement was reached on October 19, 2006, and a permanent agreement in late July 2007.

European Court of Justice Ruling

In May 2006, the European Court of Justice ruled in favor of an "action of annulment" requested by the European Parliament with regard to the legality of an agreement made by the European Commission and CBP to exchange PNR data to improve passenger prescreening for terrorists, attempting to board transatlantic flights.[113] The court ordered the cessation of PNR data sharing on September 30, 2006.[114] If it had not been resolved, this impasse between the U.S. and EU authorities with regard to PNR data sharing might have significantly affected travel from EU countries to the United States. While the European Commission and CBP renegotiated an interim agreement in terms that were not objectionable to the European Court of Justice, that agreement was temporary. Some European authorities, including Members of the European Parliament, continued to express concern about adequate data protections under the agreement.

CBP Proposed Rule Requires Additional PNR Data Preflight

In July 2006, CBP published a notice of proposed rulemaking, in which the agency sought to acquire PNR data (complete manifests) 60 minutes prior to departure, with a mechanism that would allow for individual, real-time transactions up to 15 minutes prior to a flight's departure for last-minute ticket buyers and other manifest changes.[115] In part, U.S. authorities maintain that such advanced information is necessary for prescreening noncitizens traveling to the United States under the visa waiver program, as well as long-term, multiple-entry visa holders, because they are not screened at a U.S. consulate abroad as part of a visa issuance process.[116]

---

[112] Michael Chertoff, "A Tool We Need to Stop the Next Airliner Plot," *Washington Post*, August 29, 2006, p. A15.

[113] "EU Court Rules Illegal EU-U.S. Air Passenger Data Deal," Associate Press Worldstream, May 30, 2006.

[114] "EU, US Officials: New Agreement Will Be Reached on Passenger Data," Agence France Presse, May 30, 2006.

[115] *Federal Register*, vol. 71, no. 135, July 14, 2006, pp. 40035-40048.

[116] It is noteworthy that in the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173), Congress included a requirement that countries participating in the visa waiver program issue their nationals machine-readable, tamper-resistant, biometric passports by October 26, 2004. In a subsequent law (P.L. 108-299), the machine-readable and tamper-resistant requirements were extended to October 26, 2005, and the biometric requirement was modified so that it only applied to passports issued after that date. In the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), Congress required that visa waiver countries certify that they are developing a machine-readable, tamper-resistant, biometric passport by October 26, 2006. For further information, see CRS Report RL32221, *Visa Waiver Program*, by Alison Siskin.

Following the foiled conspiracy to bomb several airliners flying from Britain to the United States in August 2006, observers noted that the suspected conspirators could have boarded the aircraft bound for the United States without having been screened against the international terrorist watchlists maintained by the TSC in the TSDB prior to a flight's departure, because the UK is a participant in the visa waiver program. In response to the plot, DHS reportedly issued a temporary order requiring that passenger name records be provided preflight to CBP for transatlantic flights originating in the UK,[117] as opposed to 15 minutes after a flight's departure as normally required under current CBP regulations (for arrival manifests).[118] Furthermore, CBP reportedly announced that it would seek to obtain greater amounts of air passenger data preflight from all air carriers and retain that data longer.[119] Reportedly, some Europeans strongly opposed such data sharing and see U.S. demands for such data, without stronger data privacy safeguards, as an infringement on their national and collective sovereignties.[120]

EU-U.S. Interim Agreement

Despite lingering concerns about data protection and privacy, on October 19, 2006, the EU and U.S. concluded an interim agreement on PNR that allows PNR data in air carrier reservations systems to continue to be transferred to CBP in the same manner as previously. It also reportedly addressed other privacy issues. For example, the agreement anticipated the development of a new screening system, under which air carriers would send (push) PNR data to CBP, rather than the air carriers allowing CBP access (pull) the data from their reservations systems, as is the case today.[121] This issue is often referred to as the "push/pull issue" and involves systems access and data control. There were additional data protection/privacy issues for the European Union and the United States to resolve in regard to TSA's Secure Flight program and CBP's Automated Targeting System. Particularly troubling for some Europeans and privacy advocates were the following proposed elements of the agreement: (1) retention of PNR data for up to 40 years; (2) collection of increased amounts and types of data; and (3) distribution of that data, along with risk assessments and possibly other analyses, to other law enforcement agencies, where control of those data would be beyond the reach of the agencies whose missions necessitated that such data be collected. The interim agreement would have expired on July 31, 2007.

EU-U.S. Permanent Agreement

On July 26, 2007, then-DHS Secretary Michael Chertoff announced a new agreement between the European Union and the United States on PNR data sharing.[122] Chertoff underscored that PNR data were an essential screening transatlantic travelers against watchlists. Under the permanent

---

[117] Mark Skertic, "Passenger List Review May Add To Flight Time," *Chicago Tribune*, August 17, 2006, p. 1.

[118] 19 *Code of Federal Regulations* (CFR), Parts 4 and 122.

[119] Ellen Nakashima, "U.S. Seeks to Expand Data Sharing: Retention of Airline Passenger Details Raises Privacy Concerns in E.U.," *Washington Post*, August 23, 2006, p. A5.

[120] Ibid.

[121] "Council Adopts Decision on Signature of Agreement with U.S. on Continued Use of PNR Data," *US Fed News*, October 16, 2006.

[122] Department of Homeland Security, Statement of Homeland Secretary Michael Chertoff On A New Agreement With The European Union For Passenger Name Record Data Sharing, Press Release, July 26, 2007.

agreement, DHS would collect 19 types of PNR data, which would be maintained for seven years in an active file and eight years in a dormant file. On August 23, 2007, DHS issued a final rule that requires all international air carriers and vessel operators to provide CBP with advanced passenger information, including PNR data, in advance of an aircraft's departure or vessel's departure/arrival, depending on the vessel's port of origin (U.S. or foreign).[123] This rule became effective on February 18, 2008.

[123] U.S. Department of Homeland Security, Bureau of Customs and Border Protection, "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels," Final rule, 72 *Federal Register*, pp. 48320-48353, August 23, 2007.

Appendix D. Secure Flight Data Elements

Secure Flight Passenger Data (SFPD) elements include the following:

- Full Name.
- Date of Birth.
- Gender.
- Redress Number or Known Traveler Number (if available).
- Passport Number (if available).
- Passport Country of Issuance (if available).
- Passport Expiration Data (if available).
- Foreign Airport Code—place of origination.
- Port of First Arrival.
- Flight Number.
- Date of Aircraft Departure.
- Time of Aircraft Departure.
- Date of Aircraft Arrival.
- Scheduled time of Aircraft Arrival.[124]

Author Contact Information

William J. Krouse
Specialist in Domestic Security and Crime Policy
wkrouse@crs.loc.gov, 7-2225

Bart Elias
Specialist in Aviation Policy
belias@crs.loc.gov, 7-7771

[124] 73 *Federal Register*, pp. 64023-64024, October 28, 2008.