Order Code RL33645

CRS Report for Congress

Terrorist Watchlist Checks and Air Passenger Prescreening

Updated January 19, 2007

William J. Krouse
Specialist in Domestic Security
Domestic Social Policy Division

Bart Elias
Specialist in Aviation Safety, Security, and Technology
Resources, Science, and Industry Division

Congressional Research Service

Prepared for Members and Committees of Congress

Terrorist Watchlist Checks and Air Passenger Prescreening

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. While screening agencies have taken some steps to ameliorate those problems, other related issues have arisen, underscoring that screening passengers for more intensive searches of their person or baggage, or to prevent them from boarding an aircraft in the event of a terrorist watchlist hit, is likely to be a difficult proposition for the federal agencies tasked with aviation and border security, principally the Department of Homeland Security (DHS), Transportation Security Administration (TSA), and Customs and Border Protection (CBP). Recent developments underscore the difficulties encountered by frontline-screening agencies.

For example, in late 2006, the DHS Privacy Office reported that TSA had not accurately described its use of personal data while testing a new air passenger prescreening system known as Secure Flight in notifications required under the Privacy Act. The Privacy Office and the Department also reported on CBP's Automated Targeting System, which assigns risk assessments to both cargo and passengers and has been operational for several years. While those reports were made in the spirit of greater government transparency, they generated additional public scrutiny and criticism.

In the 110th Congress, meanwhile, the House has passed a bill (H.R. 1) to implement further the recommendations of the 9/11 Commission on January 9, 2007. This bill includes two provisions that would require the DHS Secretary to (1) establish a timely and fair appeals process for persons delayed or prevented from boarding a commercial aircraft by any homeland security agency, and (2) formulate a strategic plan to test and implement an advanced passenger prescreening system. Congress included similar provisions in the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458).

Also, in August 2006, a foiled conspiracy to bomb airliners bound for the United States from the United Kingdom (UK) raised questions about the adequacy of existing processes to prescreen air passengers against terrorist watchlists. In response to that plot, DHS reportedly issued a temporary order requiring that passenger name records (PNRs) be provided preflight to CBP for transatlantic flights originating in the UK, as opposed to 15 minutes after the flight's departure as required previously. In addition, CBP has sought greater amounts of PNR data preflight from all air carriers and to retain that data for a greater length of time. U.S. authorities maintain that these measures are necessary to provide greater aviation and border security. In July 2006, however, the European Court of Justice ruled that the existing agreement between the European Commission and CBP to exchange PNRs was illegal. The court ordered the cessation of this data exchange on September 30, 2006. While a new agreement was reached in October 2006, this impasse could have significantly affected travel from European Union countries to the United States. Moreover, the agreement is temporary and is set to expire on July 31, 2007.

Contents

Terrorist Watchlist Checks and Air Passenger Prescreening

Introduction

Considerable controversy surrounds U.S. air passenger prescreening processes and terrorist watchlist checks. In the past, such controversy centered mainly around diverted international flights and misidentified passengers; however, the foiled conspiracy to bomb airliners bound for the United States from the United Kingdom (UK) in August 2006 raised additional questions about the adequacy of existing processes to prescreen air passengers preflight against terrorist watchlists. This report examines (1) measures taken in the wake of the 9/11 terrorist attacks to improve terrorist watchlist screening, (2) U.S. agency efforts underway to improve air passenger prescreening against those watchlists prior to departure (preflight), and (3) possible issues associated with maintaining such watchlists and prescreening air passengers, including the misidentification of persons as terrorists as the result of watchlist checks.

Recent Developments

On the terrorist watchlist and air passenger prescreening front, there have been several developments in recent months. On January 17, 2007, the head of the Department of Homeland Security (DHS) Transportation Security Administration (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).[1] With regards 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%.[2]

Hawley also 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.[3] At the departmental level, according to Hawley, DHS Secretary Michael Chertoff had also developed a program

---

[1] 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," Jan. 17, 2007.

[2] Ibid.

[3] Ibid.

envisioned by Secretary of State Condoleezza Rice that is designed to provide travelers with a single, simple process for addressing watchlist-related complaints.[4] He also testified that the advance air passenger prescreening program known as Secure Flight would reduce misidentifications — the largest source of complaints — but that program reportedly would not be up and running until at least 2008.[5]

On January 9, 2007, meanwhile, the House of Representatives passed a bill (H.R. 1), the Implementing the 9/11 Commission Recommendations Act of 2006, that includes two air passenger prescreening provisions. Those provisions would require the DHS Secretary to (1) establish a timely and fair appeals process for persons delayed or prevented from boarding a commercial aircraft by any homeland security agency, and (2) formulate a strategic plan to test and implement an advanced passenger prescreening system.

In December 2006, the DHS's Privacy Office issued a report, finding that the TSA had not accurately described its use of personal data while testing an advanced passenger prescreening system in notifications required under the Privacy Act.[6] In November 2006, the DHS Privacy Office issued a notice,[7] and the Department issued a privacy impact assessment,[8] on Customs and Border Protection's (CBP's) Automated Targeting System. Those reports and the notice generated additional public scrutiny and criticism of DHS air passenger prescreening programs and processes.[9]

In October 2006, the European Union and CBP renegotiated a passenger name record information sharing agreement, but this agreement is temporary and is set to expire on July 31, 2007.[10] In late September 2006, the Government Accountability Office (GAO) reported on U.S. government efforts to reduce the adverse effects of terrorist watchlist screening, outlining measures that DHS and the Terrorist Screening Center, which is administered by the Federal Bureau of Investigation (FBI), had

---

[4] Ibid.

[5] Beverley Lumpkin, "No-Fly List Checked for Accuracy, Cut," *Associated Press*, Jan. 18, 2007.

[6] 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*, Dec. 2006, 15 pp.

[7] 71 *Federal Register* 64543, Nov. 2, 2006.

[8] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System*, Nov. 22, 2006, 30 pp.

[9] See "Foreign Opposition Mounts to Traveler Screening Program," *National Journal's CongressDaily*, Dec. 11, 2006; Ellen Nakashima and Del Quentin Wilber, "Report Says TSA Violated Privacy Law; Passengers Weren't Told That Brokers Provided Data to Screening Program in '04," *Washington Post*, Dec. 22, 2006, p. A07; and Shaun Waterman, "Analysis: Dems Slam Border Screening Rules," *United Press International*, Jan. 2, 2007.

[10] Madhu Unnikrishnan and Martial Tardy, "EU, U.S. Strike Interim Deal On PNR Data Transfer," *Aviation Daily*, vol 366, no. 5, Oct. 9, 2006, p. 3.

undertaken to reduce and alleviate misidentifications.[11] In this report, GAO also described the U.S. government's layered approach to terrorist screening and provided analysis of the different statutory authorities, under which "frontline-screening agencies" operate.[12]

Background: HSPD-6 and Terrorist Screening

In September 2003, President Bush issued Homeland Security Presidential Directive 6 (HSPD-6), establishing a Terrorist Screening Center (TSC) to consolidate the U.S. government's approach to terrorist screening.[13] 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 TSC 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 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.[14]

Under HSPD-6, TIPOFF was officially transferred to the TTIC on September 16, 2003. Nearly a year later, President George W. Bush established the NCTC by executive order on the foundations of the TTIC.[15] The NCTC continued TTIC's efforts to establish a much more expansive database on international terrorists. Based largely on TIPOFF, the NCTC currently maintains a Terrorist Identities

---

[11] U.S. Government Accountability Office, *Terrorism Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, GAO-06-1031, Sept. 2006, p. 55.

[12] Ibid.

[13] The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, Sept. 16, 2003), available at [http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html].

[14] 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.

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

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 will be stored. According to a press account, the TIDE includes over 325,000 terrorist-related records.[16]

TSC and Terrorist Watchlisting and Screening

The TSC is a multiagency collaborative effort administered by the FBI. The NCTC shares international terrorist identities data, which is TIDE-generated, with the TSC. Combining these data with other government watchlists, the TSC has established and maintains a consolidated Terrorist Screening Database (TSDB). In addition, the TSC has developed comprehensive procedures for handling encounters with known and suspected terrorists and their supporters, and provides terrorist screening authorities with around-the-clock operational support in the event of possible terrorist encounters. According to the Department of Justice (DOJ) Office of Inspector General (OIG), as of January 2005, the TSDB included nearly 238,000 records.[17]

The TSC, in turn, distributes TSDB-generated international terrorist lookout records — along with domestic terrorist lookout records[18] — to frontline screening agencies. The TSC, for example, supports the terrorist screening activities of the DHS's TSA and CBP, as well as the DOS's Bureau of Consular Affairs (CA). Some aspects of these terrorist screening activities, however, remain controversial, particularly with regard to misidentifications (false positives).[19] Coordination between DOJ and DHS on this and other issues has proved challenging.[20]

TSA and CBP and International Air Passenger Prescreening Against Terrorist Watchlists

The foiled conspiracy to bomb airliners bound for the United States from the UK in August 2006 raised additional questions about the adequacy of existing systems to screen air passengers preflight against terrorist watchlists. Considerable controversy surrounds air passenger prescreening processes, underscoring that screening passengers for more intensive searches of their person or baggage, or to prevent them from boarding an aircraft in the event of a terrorist watchlist hit, is

---

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

[17] U.S. Department of Justice, Officer of the Inspector General, Audit Division, *Review of the Terrorist Screening Center*, Audit Report 05-27, June 2005, p. 49.

[18] Under HSPD-6, the FBI is charged with providing domestic terrorist data to the TSC.

[19] See CRS Report RL32802, *Homeland Security: Air Passenger Prescreening and Counterterrorism*, by Bart Elias, William Krouse, and Ed Rappaport.

[20] U.S. Department of Justice, Office of Inspector General, Audit Division, *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program*, Audit Report 05-34, August 2005, p. 26.

likely to be a difficult proposition for the federal agencies tasked with aviation and border security. Today, those agencies principally include DHS's TSA and CBP and the FBI-administered TSC.

TSA Air Passenger Screening

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,[21] 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).[22] Since then, the lists have been expanded almost daily.[23] 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.[24] 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

---

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

[22] National Commission on Terrorist Attacks Upon the United States, *The Aviation Security System and the 9/11 Attacks*, Staff Statement no. 3, Jan. 27, 2004, p. 6. Available at [http://www.9-11commission.gov/staff_statements/staff_statement_3.pdf].

[23] 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].

[24] 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.

per day with potential name matches.[25] During 2004, the "No Fly" and "Automatic Selectee" lists were the subject of increased media scrutiny for misidentifications. In some cases, these misidentifications included Members of Congress (e.g., Senator Edward Kennedy and Representatives John Lewis and Don Young).[26]

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.

CBP Air Passenger Prescreening

Air passengers on inbound and outbound international flights are also screened by CBP with border security systems that include a much larger subset of the TSDB-generated terrorist lookout records than those included in the "No Fly" or "Automatic Selectee" lists. Even before the 9/11 attacks, limited amounts of Passenger Name Record (PNR) data were transferred to CBP predecessor agencies (the U.S. Customs Service and the Immigration and Naturalization Service) for incoming international flights. As it was prior to the 9/11 attacks, such data are transferred to CBP from air carriers through the Advanced Passenger Information System (APIS), which runs on the legacy Treasury Enforcement Communications System (TECS).[27] PNR data are compared with several watchlists that reside on the Interagency Border Inspection System (IBIS), including the TSDB-generated terrorist watchlist.[28]

---

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

[26] 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*, Aug. 21, 2004, p. A08.

[27] APIS was developed in 1988 by the U.S. Customs Service and the Immigration and Naturalization Service. Although the electronic submission of passenger manifests through APIS was voluntary at first, most air carriers submitted their manifest electronically prior to the 9/11 attacks. Following those attacks, Congress included provisions requiring the electronic submission of manifests in the Aviation and Transportation Security Act (P.L. 107-71) and the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173).

[28] U.S. Department of State, *TIPOFF, CLASS, IBIS, CT-LINK slide show presentation*, Oct. 6, 2002, available at [http://www.markletaskforce.org/documents/TIPOFF.pdf]. U.S. Department of Homeland Security, Privacy Impact Statement for the Advance Passenger Information System (APIS), Mar. 21, 2005, p. 6, available at [http://www.dhs.gov/interweb/assetlibrary/privacy_pia_cbpapis.pdf].

In addition, PNR data are linked to other immigration inspections systems (including biometric data) as part of the US-VISIT program — the ultimate objective of which is to record the entry and exit of every noncitizen to and from the United States.[29] In the future, such data linkages and corresponding interagency information sharing could be useful to intelligence and law enforcement agencies for not only "connecting the dots," but for interdicting known or suspected terrorists at our borders as well.

Passenger Name Record Data. In FY2004, CBP sought greater amounts of PNR data from European airlines. Negotiations over acquiring such data were "highly publicized," and U.S. authorities threatened to fine the European airlines for not providing such data. In May 2004, an interim agreement was negotiated with the European Commission, under which CBP has been provided with 34 specific categories of PNR data for travelers on international flights from European Union (EU) countries. In June 2004, however, the European Parliament challenged this agreement with an "action of annulment" in the European Court of Justice.[30]

In May 2006, the European Court of Justice ruled that the existing agreement between the European Commission and CBP was illegal, on the basis that the PNR agreement was not within the competency of the commission. Consequently, the court ordered the cessation of PNR data exchange on September 30, 2006, if a new agreement was not reached that addressed the court's objections with the existing agreement.[31] It is notable that the court's decision reportedly was not founded upon any infringement of fundamental EU data protection rights.[32] Nonetheless, members of the European Parliament expressed concern about possible infringements under the agreement when they called for the "action of annulment." Despite continuing EU concerns about data protection, an interim PNR agreement was tentatively reached between the EU Commission and CBP on October 6, 2006. Unless extended, however, this agreement is set to expire on July 31, 2007.[33]

Diverted International Flights. Under current practice, PNR data are transferred through CBP's APIS several times prior to departure as it becomes available to the airlines; however, final PNR data are sometimes not transferred through APIS until after the flight has departed (wheels up). In several recent 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

---

[29] For further information, see CRS Report RL32234, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, by Lisa M. Seghetti and Stephen R. Viña.

[30] As described more fully below, the court ruled that the agreement was illegal and ordered that the exchange of PNR data should cease on September 30, 2006, if a revised agreement has not been negotiated.

[31] Martial Tardy and Adrian Schofield, "Court Scraps European Union-U.S. Data Agreement," *Aviation Daily*, May 31, 2006, vol. 364, no. 42, p. 1.

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

[33] Ibid.

have generated significant press coverage.[34] CBP's National Targeting Center (NTC) confers with TSC representatives to resolve potential watchlist matches.

Air Passenger Misidentifications. 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.[35] 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.

9/11 Commission and Air Passenger Prescreening

In July 2004, the 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,[36] and the Administration issued Homeland Security Presidential Directive 11 (HSPD-11), calling for "comprehensive terrorist-related screening procedures."[37]

Later, in December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004,[38] a law that included several provisions that authorized the NCTC and built upon earlier efforts already undertaken under HSPD-6 to improve screening of known and suspected terrorists, particularly in regard to advanced prescreening of airline passengers.[39]

---

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

[35] 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.

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

[37] The White House, *Homeland Security Presidential Directive/HSPD-11, Subject: Comprehensive Terrorist-Related Screening Procedures* (Washington, Aug. 27, 2004), available at [http://www.whitehouse.gov/news/releases/2004/08/print/20040827-7.html].

[38] P.L. 108-458, Dec. 17, 2004, 118 Stat. 3638.

[39] For further information, see CRS Report RL32802, *Homeland Security: Air Passenger Prescreening and Counterterrorism*, by Bart Elias, William Krouse, and Ed Rapport.

Integrated Terrorist Travel Strategy

Among other things, the 9/11 Commission concluded that disrupting terrorist travel was as powerful a weapon as targeting their money.[40] The 9/11 Commission found, however, that prior to the 9/11 attacks, the intelligence community[41] did not view watchlisting as integral to intelligence work.[42] To prevent future terrorist attacks, the 9/11 Commission recommended that the United States expand terrorist travel intelligence and countermeasures,[43] and that the U.S. border security 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.[44]

To increase aviation security, the 9/11 Commission recommended that the Congress and TSA give priority to screening passengers for explosives.[45] At a minimum, the 9/11 Commission recommended that all passengers referred to secondary screening be thoroughly checked for explosives.[46] 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

---

[40] 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.

[41] 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)).

[42] 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.

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

[44] Ibid., p. 387.

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

[46] Ibid., p. 393.

- air carriers be required to supply the needed information to test and implement air passenger prescreening.[47]

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, and some observers believe that some aviation security issues have not yet been adequately addressed.[48]

Efforts To Improve Air Passenger Prescreening

Prompted in part by the 9/11 Commission's recommendations, the TSA unveiled plans to discontinue the development of the controversial Computer-Assisted Passenger Prescreening System II (CAPPS II)[49] in favor of the test program dubbed "Secure Flight,"[50] but even that program has been beset with problems and has been repeatedly delayed. For example, in December 2006, the DHS's Privacy Office issued a report, finding that the TSA had not accurately described its use of personal data as part of testing Secure Flight in notifications required under the Privacy Act.[51] Nor, has CBP's passenger prescreening activities been without controversy. In November 2006, CBP issued a notice, and the Department issued a privacy impact assessment,[52] on CBP's Automated Targeting System, generating additional public scrutiny and criticism.

TSA Secure Flight Program. According to TSA, the Secure Flight program was being 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

---

[47] Ibid.

[48] 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*, Aug. 21-28, 2006, p. 50.

[49] CAPPS II was originally designed to use sophisticated algorithms to search both government and commercial databases to acquire limited background information on ticket buyers to authenticate their identity and look for irregularities in behavioral patterns that might suggest that they could pose a risk. Critics, however, decried the cloak of secrecy under which TSA developed CAPPS II and argued that the potential loss of privacy under such a system would not be counterbalanced with a corresponding increase in security. See Jill D. Rhodes, "CAPPS II: Red Light, Green Light, or 'Mother, May I?'" *The Homeland Security Journal*, March 2004, p. 1. For further discussion of CAPPS II and other aspects of air passenger prescreening, see CRS Report RL32802, *Homeland Security: Air Passenger Prescreening and Counterterrorism*.

[50] U.S. Department of Homeland Security, Transportation Security Administration, *TSA to Test New Passenger Pre-Screening System*, (Washington, Aug. 26, 2004), 2 p.

[51] Ellen Nakashima and Del Quentin Wilber, Report Says TSA Violated Privacy Law; Passengers Weren't Told That Brokers Provided Data to Screening Program in '04," *Washington Post*, Dec. 22, 2006, p. A07.

[52] Spencer S. Hsu and Ellen Nakashima, "Traveler Data Program Defied Ban, Critics Say; Congress Barred Funds for DHS Development," *Washington Post*, Dec. 9, 2006, p. A02.

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.

Domestic and International Screening. To reduce redundant or overlapping passenger processing systems, it appeared that Secure Flight would be used *only* for prescreening passengers on *domestic* flights. DHS's CBP would be responsible for checking passenger identities against watchlists and prescreening passengers on inbound and outbound *international* flights. It is unclear, however, whether responsibility for screening domestic and international flights can be clearly divided between TSA and CBP, because many international flights have domestic legs and international passengers sometimes make connections to domestic flights.

It is also unclear, moreover, whether the development of Secure Flight will impair entirely 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. Presently, the "No Fly" and "Automatic Selectee" lists are used by air carriers to screen passengers on international and domestic flights. It remains an open policy question whether this prescreening mechanism will be replaced by CBP pre-departure screening of air passengers on all in-bound international flights. In the case of international air travel, the distinction between aviation and border security functions has become increasingly blurred.

Related Provisions in the Intelligence Reform Act. Congress, meanwhile, included several air passenger prescreening-related provisions in the Intelligence Reform and Terrorist Prevention Act (P.L. 108-458). Among other things, this law requires (1) TSA to assume the airline passenger prescreening function from U.S. air carriers after it establishes an advanced passenger prescreening system for domestic flights that uses the consolidated TSDB (described as a domestic corollary system to US-VISIT); (2) CBP to prescreen passengers on international flights against the TSDB *prior to departure*; and (3) DHS to establish appeals procedures by which persons who are identified as security threats may challenge such determinations.

In addition, Congress included two reporting requirements in P.L. 108-458 related to air passenger prescreening and terrorist watchlists. The first required the DHS Privacy Officer to report to Congress on the impact of the "No Fly" and "Automatic Selectee" lists on privacy and civil liberties. The second required the National Intelligence Director to report to Congress on the criteria for placing individuals on a terrorist watchlist. Both reports were due to Congress by June 15, 2005. While the DHS Privacy Office issued its report in April 2006,[53] it is unknown whether the National Intelligence Director reported to Congress on the criteria used for placing individuals on terrorist watchlists. As the DHS Privacy Office noted, however, it is likely that such information could not be made public, without compromising national security. The Privacy Office report is discussed in greater detail below.[54]

Related Appropriations Rider. Also, in the FY2006 DHS Appropriations Act (P.L. 109-90), 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.[55] A similar provision was included in the FY2007 DHS Appropriations Act (P.L. 109-295).[56]

Problems Developing Secure Flight. Like its predecessor, CAPPS II, the Secure Flight program has proven 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.[57] 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.[58] Consequently, the GAO reported that it was uncertain whether TSA would meet its August 2005 Secure Flight operational deployment date.[59] The TSA, in fact, did not meet the deadline and in February 2006 announced that it was restructuring ("rebaselining") the Secure Flight program.

---

[53] 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.

[54] Ibid., p. 9.

[55] Sec. 518, 119 Stat. 2085.

[56] Sec. 514, 120 Stat. 1379.

[57] 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.

[58] 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, Mar. 28, 2005, p. 17.

[59] Ibid.

In addition, in July 2005, GAO reported that TSA had not fully disclosed its use of passenger data during the testing for Secure Flight.[60] In August 2005, the DOJ OIG reported that there were numerous problems coordinating the development of the Secure Flight program with the efforts of the FBI-administered TSC.[61] 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.[62] 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.[63]

Recent House-Passed Provision in the 110th Congress. On January 9, 2007, the House of Representatives passed a bill to implement further the recommendations of the 9/11 Commission. This bill (H.R. 1) includes a provision (section 409) that would require the DHS Secretary to formulate, within 90 days of enactment, a strategic plan to test and implement an advanced passenger prescreening system, with which DHS would assume the function of comparing passenger information to the "No Fly" and "Automatic Selectee" lists from air carriers, as recommended by the 9/11 Commission. It requires further that this plan include a projected timeline for testing and implementing such a system, and that it explain how this system will be integrated with the prescreening system for passengers on international flights. As described above, the head of TSA, Assistant Secretary Kip Hawley, testified before the Senate Committee on Commerce, Science and Transportation that the agency's advanced air passenger prescreening program (Secure Flight) reportedly would not be running until at least 2008.[64]

CBP's Automated Targeting System. In recent months, CBP's Automated Targeting System has also generated controversy. In early November 2006, the DHS Privacy Office issued a system of records notice (SORN) on the Automated Targeting System (ATS),[65] in compliance with the Privacy Act. Later

---

[60] U.S. Government Accountability Office, *Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public*, GAO-05-864R, July 22, 2005, p. 9.

[61] 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, Aug. 2005, 41 pp.

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

[63] 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*, Dec. 2006, 15 pp.

[64] Beverley Lumpkin, "No-Fly List Checked for Accuracy, Cut," *Associated Press Online*, Jan. 18, 2007.

[65] Federal Register, vol. 71, no. 212, Nov. 2, 2006, p. 64543.

that month, DHS published a privacy impact assessment on that system as well.[66] Initially, the effective date on this SORN was December 4, 2006, but DHS extended it to December 29, following a ground swell of public criticism.[67]

According to one news account, the U.S. Customs Service developed the ATS in the mid-1990s as a tool to assist border inspectors with interdicting illegal drugs and other contraband.[68] Arguably, then the scope of the ATS was 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. After the 2001 terrorist attacks, the ATS was reportedly reconfigured and its scope widened to target known and suspected terrorists and terrorist activities as well, by assigning risk assessments to passengers and cargo.[69] In response to the recent SORN and Privacy Office report, privacy advocates, civil libertarians, and others quickly questioned whether the development of ATS was subject to the same appropriations limitation (described above) as the Secure Flight program,[70] but DHS maintains that it was and is not subject to that limitation, as the ATS predates the Secure Flight program and, hence, cannot be viewed as a "follow on" or "successor" program to Secure Flight.[71]

Notwithstanding interpretations of the funding limitation, then Chairman-Designate of the House Committee on Homeland Security, Representative Bennie Thompson, and others have raised additional questions regarding the ATS and its impact on privacy, civil liberties, and civil rights.[72] In comments addressing the ATS SORN released on December 29, 2006, Representative Thompson expressed several concerns regarding aspects of ATS and air passenger prescreening that, in his view, would require further elaboration or revision.[73] He acknowledged the need to ensure aviation security by screening for terrorists through name-based systems; however, he emphasized that such systems "must not go beyond the letter or intent of the law

---

[66] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Automated Targeting System*, Nov. 22, 2006, 30 pp.

[67] "Senators Question Program That Put Risk Ratings On All Who Cross U.S. Borders," *COMMWEB*, Dec. 4, 2006.

[68] Spencer S. Hsu and Ellen Nakashima, "Traveler Data Program Defied Ban, Critics Say; Congress Barred Funds for DHS Development," *Washington Post*, Dec. 9, 2006, p. A02.

[69] Ibid.

[70] Ibid.

[71] U.S. Department of Homeland Security, U.S. Customs and Border Protection, "Facts Concerning the Automated Targeting System," December 12, 2007, available at [http://www.cbp.gov/xp/cgov/newsroom/highlights/cbp_responds/facts_automated_targeting_sys.xml].

[72] Shaun Waterman, "Analysis: Dems Slam Border Screening Rules," *UPI*, Jan. 2, 2007.

[73] "Comments of Rep. Bennie G. Thompson (D-MS), Chairman-Designate Committee on Homeland Security, U.S. House of Representatives, on Department of Homeland Security Privacy Office Privacy Act System of Records Notice for the U.S. Customs and Border Protection Automated Targeting System (Docket No. DHS-2006-0060, Published Nov. 2, 2006, Extended December 8, 2006)," Dec. 29, 2006, 7 pp.

by infringing upon the guaranteed rights of U.S. Citizens."[74] He also noted concerns about the type of data collected from PNRs and the ways in which that data collected on U.S. citizens and legal permanent residents would be analyzed, protected, shared, controlled, and retained.[75]

In addition, the EU Commissioner for Justice, Freedom, and Security, Mr. Franco Frattini, was quoted in the press as having made the following statement on December 13, 2006 regarding the ATS: "the information published by the DHS reveals significant differences between the way in which PNR data are handled with the ATS on the one hand and the stricter regime for European PNR data according to the [October 19, 2006] interim agreement"[76] (described below).

TSC Operations and Support for Secure Flight

Regarding TSC operations and support for the Secure Flight program, the DOJ OIG issued two audits in the summer of 2005. Congress, meanwhile, provided the TSC with increased funding to support the Secure Flight program, among other terrorist screening initiatives. Nevertheless, TSA has encountered difficulties in adequately developing the program, and its implementation has been repeatedly delayed.

Inspector General Audit of TSC Operations

In June 2005, DOJ OIG issued an audit, reporting that the TSC had established a single consolidated TSDB, as recommended by GAO,[77] but with some difficulties.[78] Among other things, the TSDB had not been completely audited to ensure that its records were complete and accurate. The OIG also reported that the NCTC was using TIPOFF as the principal source of lookout records for international terrorists, and the TIDE was slated to be brought online in mid-2005.[79] During a Senate hearing on passport fraud, the TSC Director, Donna Bucella, testified that the TIDE had been "incorporated" into the TSDB.[80]

---

[74] Ibid.

[75] Ibid.

[76] "European Commissioner Issued A Statement Saying That The U.S. Homeland Security Department Deviated From Recent Agreements Between the US and EU," *TECHWEB*, Dec. 20, 2006.

[77] 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).

[78] 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.

[79] Ibid., p. 6.

[80] Statement of Donna A. Bucella Director, Terrorist Screening Center, before the Senate Committee on Homeland Security and Governmental Affairs, Hearing on Passport (continued...)

NCTC Support of TSC Watchlisting. An oversight issue for Congress — some may maintain the most critical issue — is whether the Intelligence Community is sharing reliable information with the NCTC that is necessary to identify effectively known and suspected terrorists and their supporters. Because TIDE-generated records are the principal source of watchlist records on international terrorists, this issue undergirds the TSC's ability to accomplish its mission. To date, the Office of the Director of National Intelligence OIG has not reported an audit of the NCTC's support of the TSC, nor is it publically known whether the NCTC has evaluated the TIDE for accuracy and comprehensiveness.

Anticipated FY2006 TSC Support for Secure Flight

In August 2005, the DOJ OIG issued an audit of the TSC's support for the Secure Flight program, reporting that such support would significantly increase the TSC's workload.[81] The FBI-administered TSC anticipated that supporting the Secure Flight program and other terrorist screening initiatives would increase the number of possible terrorist encounters by 500% in FY2006, compared with its estimated FY2005 workload.[82] The Administration had requested $75 million to fund an additional 61 positions for the TSC as part of the overall FBI request,[83] bringing the total FY2006 request for the TSC to nearly $99 million, according to the DOJ OIG. Of the latter amount, the OIG reported that about 40% was either directly or indirectly attributable to the TSC's anticipated support of TSA's Secure Flight program.

The FY2006 Science-State-Justice-Commerce appropriations bill (H.R. 2862) included conference report language that earmarked a $70 million increase for the TSC to fund an additional 61 positions.[84] With this increased funding, the TSC was in a position financially to support the Secure Flight program. In February 2006, however, GAO testified before the Senate Commerce, Science, and Transportation Committee that TSA still faced significant program development challenges. Shortly thereafter, the TSA put Secure Flight on hold so that the program could be redesigned (rebaselined).[85]

---

[80] (...continued)
Vulnerabilities, Washington, June 29, 2005, p. 2.

[81] 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, (Washington, Aug. 2005), 41 pp.

[82] U.S. Department of Justice, *2006 Congressional Authorization & Budget Submission*, vol. II, Federal Bureau of Investigation (Washington, Febrary 2005), pp. 3-33.

[83] Ibid.

[84] H.Rept. 109-272, conference report on the FY2006 SSJC appropriations act (H.R. 2862), which was enacted as P.L. 109-108.

[85] U.S. Government Accountability Office, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, Statement of Cathleen A. Berrick, GAO-06-374T, Feb. 9, 2006.

EU-U.S. Data Sharing Issues

In Summer 2006, the issue of PNR data sharing emerged as a problem for the United States, as the European Court of Justice has ruled an EU-U.S. PNR data sharing agreement to be illegal and ordered a cessation of such data sharing on September 30, 2006. In light of the foiled plot to bomb airliners flying from the UK to the United States in August 2006, however, DHS Secretary Chertoff proposed that the United States should acquire greater amounts of PNR data to improve passenger prescreening for known and suspected terrorists.[86] As described below, an interim EU-U.S. agreement was reached on October 19, 2006.

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.[87] The court ordered the cessation of PNR data sharing on September 30, 2006.[88] 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 is temporary. And, some European authorities, including Members of the European Parliament, continue to express concern about adequate data protections under the agreement.

CBP 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.[89] In part, U.S. authorities maintained 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.[90]

---

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

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

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

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

[90] It is noteworthy that in the Enhanced Border Security and Visa Entry Reform Act of 2002 (continued...)

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,[91] as opposed to 15 minutes after a flight's departure as normally required under current CBP regulations (for arrival manifests).[92] 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.[93] Reportedly, some Europeans strongly oppose 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.[94]

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 addresses other privacy issues. For example, the agreement anticipates the development of a new screening system, under which air carriers will 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.[95] This issue is often referred to as the "push/pull issue" and involves systems access and data control.

Nonetheless, there may be additional data protection/privacy issues for the European Union and the United States to resolve in regard to air passenger

---

[90] (...continued)
(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.

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

[92] 19 *Code of Federal Regulations* (CFR), Parts 4 and 122.

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

[94] Ibid.

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

prescreening under both TSA's Secure Flight program and CBP's Automated Targeting System. Particularly troubling for some Europeans and privacy advocates are the following 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 these data would be beyond the reach of the agencies whose missions necessitated that such data be collected. The interim agreement is due to expire on July 31, 2007.

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.[96]

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 Administration maintains further that since the TSC does not 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

---

[96] 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).

in written documents (operational guidelines).[97] Congress later required reports from the Administration and GAO regarding the use of terrorist watchlists.

DHS Privacy Office Report on "No Fly" and "Automatic Selectee" Watchlists

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,[98] 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.[99] The report cited concerns about the quality of the information of those lists, as well as the underlying intelligence.[100] 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.[101] 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

---

[97] Ibid., p. 76.

[98] 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.

[99] 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.

[100] Ibid., p. 8.

[101] Ibid., p. 9.

and security, or (2) allowing persons wishing to avoid detection to subvert those lists.[102]

GAO Report on the Adverse Effects of Terrorist Watchlists

In late September 2006, GAO reported on efforts to reduce the adverse effects of terrorist watch list screening, outlining measures that DHS and the TSC had taken to reduce and alleviate misidentifications.[103] According to GAO, the TSC established formal internal procedures for receiving and processing redress matters in January 2005,[104] and the DOJ had drafted an interagency memorandum of understanding (MOU) to document formally redress opportunities and clarify TSC and frontline-screening agency responsibilities.[105] A final draft of the redress MOU was scheduled for interagency clearance by the fall 2006.[106]

GAO also noted that the TSC generally handles redress cases related to persons who may have been mistakenly placed on terrorist watchlists, as opposed to misidentifications, which are generally handled by the frontline-screening agencies (principally CBP and TSA).[107] During calendar year 2005, the TSC processed 112 redress cases to completion:

- 31 involved individuals mistakenly watchlisted,
- 48 required no change to the record,
- 6 involved changes or updates to the record,
- 8 were not relevant to watchlist issues and should not have been referred to the TSC, and
- 19 involved misidentifications that should have been handled by the frontline-screening agencies.

GAO also noted that while the total number of misidentifications by frontline-screening agencies is unknown, their frequency, while a very small percentage of

---

[102] Ibid.

[103] U.S. Government Accountability Office, *Terrorism Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, GAO-06-1031, Sept. 2006, p. 55.

[104] Ibid., p. 29.

[105] Ibid., p. 27.

[106] Ibid.

[107] It is notable that consular officers are given wide discretion whether to grant or refuse a visa. Their decisions are subject to limited review, and there are no avenues for administrative appeal. Moreover, a visa (immigrant or nonimmigrant) is not a guarantee of entry into the United States. CBP inspectors at ports of entry may find cause to exclude a visaed alien form entry, although this seldom occurs. See CRS Report RL31019, *Terrorism: Automated Lookout Systems and Border Security Options and Issues*, by William J. Krouse and Raphael F. Perl.

total inspections, is estimated to be in the tens-of-thousands and remains a serious concern.[108]

DHS Redress Mechanisms

In the reports discussed above, both the DHS Privacy Office and GAO reported to Congress on existing DHS redress mechanisms, by which an individual that feels he or she has been unfairly denied boarding on a commercial aircraft or singled out for screening, can contact several DHS offices and initiate a redress inquiry. More recently, Congress has considered legislation to establish a single office to oversee the DHS's redress processes, and the head of TSA has testified before Congress about new efforts to improve those processes.

Existing Mechanisms. According to the DHS Privacy Office, individuals who believe they have been misidentified as a terrorist while being screened by TSA can contact either the TSA Ombudsman's Contact Center or Office of Civil Rights.[109] Information is also available on the TSA website regarding the redress process.[110] Individuals seeking redress are issued a Privacy Act Notice and Passenger Identity Verification Form, which is processed by the TSA Office for Transportation Security Redress (OSTR).[111] If OSTR concludes an individual has been misidentified, they are placed on a "cleared" list.[112] However, GAO has reported that individuals, who have been placed on the cleared lists, may continue 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."[113]

Meanwhile, individuals who believe they have been misidentified while being screened by CBP can contact that agency's Customer Service Satisfaction Unit.[114] In addition to contacting either TSA or CBP, individuals who have possibly been misidentified may also contact either the DHS Privacy Office or Office of Civil Rights and Civil Liberties.[115] As described above, frontline-screening agencies refer matters concerning individuals who believe they have been mistakenly watchlisted to the TSC.

---

[108] Ibid., p. 12.

[109] 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.

[110] Ibid.

[111] Ibid.

[112] Ibid.

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

[114] 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.

[115] Ibid.

Recent House-Passed Provision in the 110th Congress. The House passed a bill (H.R. 1) to implement further the 9/11 Commission's recommendations. H.R. 1 includes a provision (section 407) that would require the DHS Secretary to establish an Office of Appeals and Redress at the departmental level, under which a timely and fair process would be established to allow individuals who believe they have been wrongly delayed or prohibited from boarding a commercial aircraft by either the TSA or CBP to appeal those actions and seek redress. In developing those procedures, however, individuals seeking redress from either DHS or the FBI-administered TSC may encounter significant statutory hurdles.

Senate Hearing on Aviation Security. At a recent hearing held by the Senate Committee on Commerce, Science and Transportation, the 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.[116] Hawley also testified that DHS Secretary Chertoff had developed a program envisioned by Secretary of State Condoleezza Rice that is designed to provide travelers with a single, simple process for addressing watchlist-related complaints.[117]

Hawley also testified that the advance air passenger prescreening program known as Secure Flight would reduce misidentifications — the largest source of complaints.[118] 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.[119] In addition, Hawley informed the committee that TSA and the FBI-administered TSC were in the process of reviewing the "No Fly" list in an effort to reduce the number of individuals on that list by as much as 50%.[120]

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.[121] 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

---

[116] 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," Jan. 17, 2007.

[117] Ibid.

[118] Ibid.

[119] Ibid.

[120] Ibid.

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

testimony, 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. Director Bucella suggested that the TSC would probably be unable to confirm or deny whether the person was in the TSDB under current law.[122]

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,[123] 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, for records indicating they are 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.[124] 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[125] 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 their administrative remedies prior to bringing an action in U.S. District Court to challenge the agency's action.[126]

Other Possible Legal Questions

The Administration has pledged that terrorist screening information will be gathered and employed within constitutional and other legal parameters. Although the Privacy Act generally does not restrict information sharing related to known and

---

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

[123] 5 U.S.C. §522.

[124] 5 U.S.C. §§522(b), (c), 522a(j).

[125] 5 U.S.C. §522a.

[126] 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

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 on-going foreign intelligence or criminal investigations.[127] 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.

Possible Issues for Congress

Four 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? How accurate and complete is the consolidated terrorist screening database itself? 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 database (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 whether the intelligence community is 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?

Accuracy and Completeness of the Terrorist Screening Database

According to the DOJ OIG, the TSC struggled to develop a consolidated terrorist screening database, as illustrated by the several versions of this database referenced in the OIG audit and numerous problems associated with the database. Among other things, the problems included data inaccuracies, omitted and unactivated fields, and duplicate records in two early versions of this database. Although the TSC did manage to upload terrorist lookout records into the National Crime Information Center's system, so that it would be available to state, local, and tribal police for the first time, another issue may be whether there was a degradation in the quality of lookout records provided to other mainline screening agencies, such as the Department of State's Bureau of Consular Affairs and DHS's Customs and

---

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

Border Protection. Consequently, an issue for Congress may be whether the TSC was able to maintain the same quality of lookout records that were provided previously by the State Department's Bureau of Intelligence and Research, as there may be outstanding issues related to the accuracy and completeness of the lookout records in the consolidated terrorist screening database.

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? Will DHS and CBP be able to negotiate a permanent agreement with the EU for a greater amount of PNR data that would be provided preflight? If such an agreement cannot be reached, what will the implications be if DHS and CBP require such data through new regulations (administratively) and subsequently refuse non-compliant air carriers entry into the United States or fine them for not providing such data preflight?

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?