Order Code RL33645

CRS Report for Congress
Received through the CRS Web

Terrorist Watchlist Checks and Air Passenger Prescreening

September 6, 2006

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

Terrorist Watchlist Checks and Air Passenger Prescreening

Summary

Considerable controversy surrounds U.S. air passenger prescreening and terrorist watchlist checks. In the past, such controversy centered around diverted international flights and misidentified passengers. More recently, however, the foiled conspiracy to bomb airliners bound for the United States from the United Kingdom (UK) has raised questions about the adequacy of existing processes to prescreen air passengers against terrorist watchlists.

Observers have noted that the suspected conspirators may have been able to board aircraft bound for the United States without having been screened against the consolidated terrorist screening database (TSDB) maintained by the U.S. government prior to the flight's departure. Many of those observers have also noted that because the UK is a participant in the visa waiver program, British nationals are able to visit the United States temporarily for business or pleasure without acquiring a visa at a U.S. consular post abroad — a process during which they would be screened against the TSDB. Although all ticket purchasers are screened against aviation security watchlists (the "No Fly" and "Automatic Selectee" lists) at the point of purchase by air carriers, some international air passengers may not be screened against the larger, consolidated TSDB by U.S. border security officials prior to a flight's departure (wheels up) if they purchased their tickets just prior to the gates closing on a flight.

In response to the recent plot, the Department of Homeland Security (DHS) has reportedly issued a temporary order requiring that passenger name records (PNRs) be provided preflight to Customs and Border Protection (CBP) for transatlantic flights originating in the UK, as opposed to 15 minutes after the flight's departure as normally required under current law. In addition, CBP is seeking 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. Some Europeans, however, strongly oppose such data sharing and view U.S. demands for such data, without data privacy safeguards, as an infringement on their national and collective sovereignties. Complicating matters further, in July 2006, the European Court of Justice ruled that the existing agreement between the European Commission and CBP to exchange passenger name records was illegal. The Court ordered the cessation of this data exchange on September 30, 2006, in the absence of a new agreement that addresses the Court's objections with the existing agreement. If not resolved, this impasse could significantly affect travel from European Union countries to the United States.

The continuing controversy surrounding U.S. air passenger prescreening processes and terrorist watchlist checks underscores 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. These agencies include DHS's Transportation Security Administration (TSA) and CBP, as well as the Terrorist Screening Center, which is administered by the Federal Bureau of Investigation.

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 recently foiled conspiracy to bomb airliners bound for the United States from the United Kingdom (UK) has raised questions about the adequacy of existing processes to prescreen air passengers against terrorist watchlists. This report examines (1) measures taken in the wake of the 9/11 terrorist attacks to improve terrorist watchlists, (2) U.S. agency efforts underway to better screen air passengers 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.

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.[1] 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

---

[1] 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].

DOS's INR.[2] TIPOFF was transferred to TTIC under HSPD-6. Based largely 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 will be stored. According to a press account, the TIDE includes over 325,000 terrorist-related records.[3]

TSC and Terrorist Watchlisting and Screening

The TSC is a multiagency collaborative effort administered by the Federal Bureau of Investigation (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.[4]

The TSC, in turn, distributes TSDB-generated international terrorist lookout records — along with domestic terrorist lookout records[5] — to other screening agencies. The TSC, for example, supports the terrorist screening activities of the Department of Homeland Security's (DHS's) Transportation Security Administration (TSA) and Customs and Border Protection (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).[6] Coordination between DOJ and DHS on this and other issues has proved challenging.[7]

---

[2] 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.

[3] 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.

[4] 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.

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

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

[7] 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

(continued...)

TSA and CBP and International Air Passenger Prescreening Against Terrorist Watchlists

The recent foiled conspiracy to bomb airliners bound for the United States from the UK has raised questions about the adequacy of existing systems to prescreen air passengers 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 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,[8] 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).[9] Since then, the lists have been expanded almost

---

[7] (...continued)
05-34, August 2005, p. 26.

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

[9] 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].

daily.[10] 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.[11] 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.[12] 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).[13]

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

---

[10] 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].

[11] 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.

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

[13] 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.

the legacy Treasury Enforcement Communications System (TECS).[14] PNR data are compared with several watchlists that reside on the Interagency Border Inspection System (IBIS), including the TSDB-generated terrorist watchlist.[15]

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.[16] 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.[17] In May 2006, the European Court of Justice ruled that the existing agreement between the European Commission and CBP was illegal.[18] The Court ordered the cessation of this data exchange on September 30, 2006, if a new agreement has not been reached that addresses the Court's objections with the existing agreement.[19]

Diverted International Flights. Under current practice, PNR data are transferred through CBP's APIS several times prior to departure as it becomes

---

[14] 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).

[15] 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].

[16] 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.

[17] 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.

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

[19] Ibid.

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 have generated significant press coverage.[20] 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.[21] Despite these difficulties, the National Commission on Terrorist Attacks upon the United States (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 Final Report 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,[22] and the Administration issued Homeland Security Presidential Directive 11 (HSPD-11), calling for "comprehensive terrorist-related screening procedures."[23] Later, in December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004,[24] a law that included several provisions that authorized the NCTC and built upon earlier efforts already undertaken under HSPD-6 to better

---

[20] 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.

[21] 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.

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

[23] 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].

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

screen known and suspected terrorists, particularly in regard to advanced prescreening of airline passengers.[25]

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.[26] The 9/11 Commission found, however, that prior to the 9/11 attacks, the intelligence community[27] did not view watchlisting as integral to intelligence work.[28] To prevent future terrorist attacks, the 9/11 Commission recommended that the United States expand terrorist travel intelligence and countermeasures,[29] 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.[30]

To increase aviation security, the 9/11 Commission recommended that the Congress and TSA give priority to screening passengers for explosives.[31] At a minimum, the 9/11 Commission recommended that all passengers referred to secondary screening be thoroughly checked for explosives.[32] 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 better screen air passengers, the 9/11 Commission recommended that

- the "no-fly" and "automatic selectee" watchlists used to screen air passengers be improved without delay;

---

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

[26] 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.

[27] 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)).

[28] 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.

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

[30] Ibid., p. 387.

[31] 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.

[32] Ibid., p. 393.

- 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.[33]

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.[34]

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)[35] in favor of the test program dubbed "Secure Flight."[36]

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

---

[33] Ibid.

[34] 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.

[35] 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.*

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

- 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 has 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 air passenger prescreening-related provisions in the Intelligence Reform and Terrorist Prevention Act (P.L. 108-458) that require (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.

Related Appropriation Rider. Also, in the FY2006 DHS Appropriations Act (P.L. 109-90), Congress prohibited TSA from spending any appropriated funds on the deployment of Secure Flight, or any successor system, until the Government Accountability Office (GAO) reports that certain conditions have been met, including the establishment of an appeals process.[37]

---

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

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.[38] 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.[39] Consequently, the GAO reported that it was uncertain whether TSA would meet its August 2005 Secure Flight operational deployment date.[40] 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.[41] In August 2005, moreover, DOJ OIG reported that there were numerous problems coordinating the development of the Secure Flight program with the efforts of the FBI-administered TSC.[42] 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.[43]

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 was indefinitely postponed in February 2006.

---

[38] 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.

[39] 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.

[40] Ibid.

[41] 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.

[42] 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.

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

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,[44] but with some difficulties.[45] 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.[46] During a Senate hearing on passport fraud, the TSC Director, Donna Bucella, testified that the TIDE had been "incorporated" into the TSDB.[47]

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 effectively identify 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.[48] 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.[49] The Administration had requested $75 million to fund an additional 61 positions for the TSC as part of the overall FBI request,[50] bringing the total FY2006 request for the TSC to nearly $99 million, according to the DOJ OIG.

---

[44] 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).

[45] 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.

[46] Ibid., p. 6.

[47] Statement of Donna A. Bucella Director, Terrorist Screening Center, before the Senate Committee on Homeland Security and Governmental Affairs, Hearing on Passport Vulnerabilities, Washington, June 29, 2005, p. 2.

[48] 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.

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

[50] Ibid.

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.[51] 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).[52]

Emerging EU-U.S. Data Sharing Issues

More recently, the issue of PNR data sharing has reemerged as a problem for the United States, as the European Court of Justice has ruled a 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 a recently foiled plot to bomb airliners flying from the UK to the United States, DHS Secretary Michael Chertoff has proposed that the United States should acquire greater amounts of PNR data to better screen for known and suspected terrorists.[53]

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 in regard to the legality of an agreement made by the European Commission and CBP to exchange passenger name records to better screen for terrorists boarding transatlantic flights.[54] Although the European Commission has been working with CBP to renegotiate this agreement in terms that will not be objectionable to the European Parliament or Court of Justice, the sharing of these data under the annulled agreement is to cease on September 30, 2006.[55] If not resolved, this impasse between the U.S. and EU authorities with regard

---

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

[52] 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.

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

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

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

to PNR data sharing may significantly affect travel from EU countries to the United States.

CBP Seeks Greater Passenger Data

In July 2006, CBP published a notice of proposed rulemaking, in which the agency seeks 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.[56] 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.[57]

Following the recent foiled conspiracy to bomb several airliners flying from Britain to the United States, 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 this, DHS has reportedly issued a temporary order requiring that passenger name records be provided preflight to CBP for transatlantic flights originating in the UK,[58] as opposed to 15 minutes after a flight's departure as normally required under current CBP regulations (for arrival manifests).[59] Furthermore, CBP reportedly announced recently that it will seek to obtain greater amounts of air passenger data preflight from all air carriers and retain that data longer.[60] 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.[61]

---

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

[57] 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.

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

[59] 19 *Code of Federal Regulations* (CFR), Parts 4 and 122.

[60] 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.

[61] Ibid.

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.[62]

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 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. 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 OIG audit on TSC operations, meanwhile, included a recommendation that the TSC strengthen procedures for handling misidentifications and articulate those procedures formally in written documents (operational guidelines).[63] Although formal internal procedures for receiving and processing redress matters have been reportedly established at the TSC, there have been no public reports outlining and evaluating those procedures since the OIG audit.[64] In developing those procedures further, the TSC and other screening agencies may encounter several significant statutory hurdles as well.

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

---

[62] 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).

[63] Ibid., p. 76.

[64] Ibid., p. 137.

(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.[65] 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, 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.[66]

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,[67] 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.[68] 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[69] 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.

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

---

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

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

[67] 5 U.S.C. §522.

[68] 5 U.S.C. §§522(b), (c), 522a(j).

[69] 5 U.S.C. §522a.

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.[70] 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 effectively prescreen 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 effectively 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

---

[70] 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 an 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?