Order Code RL32802

CRS Report for Congress
Received through the CRS Web

Homeland Security: Air Passenger Prescreening and Counterterrorism

March 4, 2005

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

William Krouse
Specialist in Domestic Security
Domestic Social Policy Division

Ed Rappaport
Analyst in Social Legislation
Domestic Social Policy Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
04 MAR 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Homeland Security: Air Passenger Prescreening and Counterrorism	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library and Knowledge Repository Defense Acquisition University Fort Belvoir, VA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**34**	

Homeland Security: Air Passenger Prescreening and Counterterrorism

Summary

The adequacy of existing systems to screen air passengers against terrorist watch lists has been questioned, most notably by the 9/11 Commission. Yet, considerable controversy surrounds air passenger prescreening systems, such as the "No Fly" or "Automatic Selectee" lists, underscoring that screening passengers for more intensive searches of their persons or baggage, or to prevent them from boarding an aircraft in the event of a terrorist watch list hit, is likely to be a difficult proposition for the federal agencies tasked with aviation security. Today, those agencies principally include the Department of Homeland Security's (DHS's) Transportation Security Administration (TSA) and Customs and Border Protection (CBP), and the Federal Bureau of Investigation (FBI)-administered Terrorist Screening Center (TSC).

In October 2004, TSA unveiled the Secure Flight test program — the next generation domestic air passenger prescreening system. Secure Flight consists of four elements: (1) a streamlined rule for more intensive screening; (2) an identity authentication process; (3) a passenger name check against the consolidated terrorist screening database (TSDB); and (4) an appeals process for passengers who may have been misidentified. The TSC has consolidated the "No Fly" and "Automatic Selectee" lists with the TSDB. Since CBP has assumed responsibility for prescreening passengers on inbound and outbound international flights, TSA will only prescreen domestic flights under Secure Flight. The Administration has proposed creating an Office of Screening Coordination and Operations (SCO) — under DHS's Border and Transportation Security Directorate — to oversee Secure Flight, among other screening, expedited inspection, and credentialing programs.

Congress included provisions in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) requiring: (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 utilizes the consolidated TSDB; (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. Also, in the FY2005 DHS Appropriations Act (P.L. 108-334), Congress prohibited TSA from spending any appropriated funds on the deployment of CAPPS II, Secure Flight, or any successor system, until the Government Accountability Office reports that certain conditions have been met, including the establishment of an appeals process.

Several issues may emerge for Congress. To what extent is the FBI-administered TSC supporting the air passenger screening activities of both the TSA and CBP? Has the quality and quantity of the records on the "No Fly" list been improved? Will the TSA and CBP be able to divide cleanly responsibility for screening air passengers on domestic and international flights, respectively? Will the proposed SCO be an effective mechanism to coordinate multiple border and transportation security screening programs? When will TSA be able to deploy an advanced air passenger screening system and assume the day-to-day administration of the "No Fly" lists from the airlines?

Contents

Introduction 1

Background on Civil Aviation Passenger Prescreening 3
"No Fly" and "Automatic Selectee" Watch Lists 3
Other U.S. Government Terrorist Watch Lists 4
Computer-Assisted Aviation Prescreening System (CAPS) 6
Computer-Assisted Passenger Prescreening System II (CAPPS II) 7

Secure Flight Test Program 9
Streamlined Rule for Automatic Screening 9
Identity Authentication (IDA) 10
Watch List Checks 10
Proposed TSA Passenger Advocacy and Redress Policy 11

Border and Transportation Security Screening Coordination 12

Key Operational Considerations 13
Type I and Type II Error Tradeoffs 14
False Negatives 14
False Positives 14
Limits of Intelligence 15
Congressional Requirements 15
Balancing Benefits and Risks 15
Redress and Remedy 16
Watch List Consolidation at FBI-Administered TSC 16
Which Agency Will Handle Passenger Appeals: TSA, TSC, or Other? 17
Disclosure Under FOIA and Privacy Act 17
Other Possible Legal Questions 18
Congressional Requirements 18
Systems Integrity, Access, and Data Retention 19
Systems Platform and Infrastructure 19
Registered Traveler Pilot Program 20
Prescreening in Other Transportation Modes 21
Avoiding "Mission Creep" 21
Augmenting Prescreening with Behavioral-Based Evaluations 22
Fitting into the Larger Strategy 22

Possible Issues for Congress 23

Conclusion 24

Appendix A. Related Provisions Included in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) 26
Advanced Airline Passenger Prescreening System 26
Prescreening of Airport Employees and Others 27
Chartered and Leased Aircraft Customer Prescreening 27

Appeal Procedures 27
International Passenger Prescreening 28
Report on Effects on Privacy and Civil Liberties 28
Report on Criteria for Inclusion in the Consolidated TSDB 28
Foreign Air Marshal Trainees Prescreening 29
Maritime Vessel Passenger Prescreening 29

Appendix B. Frequently Used Abbreviations 30

Homeland Security: Air Passenger Prescreening and Counterterrorism

Introduction

Beginning in the early 1990s, civil aviation passenger prescreening consisted of the airlines checking the names of passengers against a "No Fly" list of individuals that posed a "known threat to civil aviation." This relatively small list — less than 20 individuals on September 11, 2001 — was compiled by the Federal Bureau of Investigation (FBI) and distributed to U.S. air carriers by the Federal Aviation Administration (FAA) in the form of security directives. In 1996, in response to the threat of aircraft bombings, the FAA began developing a computer-assisted aviation prescreening system (CAPS) to select passengers based on certain characteristics (which reportedly did not include race, nationality, or religious beliefs) for more intensive luggage searches. Following the 9/11 attacks, this system was modified to select passengers for more intensive searches of their persons as well, and it was renamed the computer-assisted passenger prescreening system (CAPPS). In addition, the Transportation Security Administration (TSA) — established by the Aviation and Transportation Security Act[1] — began developing a second generation computer-assisted passenger prescreening system (CAPPS II), which has generated considerable controversy.

More recently, the 9/11 Commission made several recommendations regarding aviation security and air passenger prescreening. While the Commission did not comment extensively upon CAPPS or CAPPS II, it did recommend that air passengers should be more comprehensively screened against terrorist watch lists. The four related recommendations include the following:

- improving the "no-fly" and "automatic selectee" lists without delay;
- transferring the actual screening process from U.S. air carriers to TSA;
- screening passengers against the larger set of terrorist watch lists; and
- requiring air carriers to supply needed information to test and implement passenger pre-screening.[2]

Prompted in part by these recommendations, TSA unveiled plans to discontinue the development of the controversial CAPPS II system in favor of the test program

---

[1]P.L. 107-71, 115 Stat. 597.

[2]The Commission also recommended that the Congress and TSA give priority to screening passengers for explosives. 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.

dubbed "Secure Flight."[3] According to TSA, the Secure Flight program is being designed to better deter, detect, and prevent known or suspected terrorists from boarding commercial flights. The TSA endeavors 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. As discussed below, the Secure Flight program is an amalgam of the existing CAPPS, the proposed CAPPS II system, and consolidated watch list checks.

To reduce redundant or overlapping passenger processing systems, it appears that Secure Flight will *only* be used for prescreening passengers on *domestic* flights. DHS's Customs and Border Protection (CBP) currently has responsibility for checking passenger identities against watch lists 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, as many international flights have domestic legs. The Administration, meanwhile, has proposed creating an Office of Screening Coordination and Operations (SCO) — under DHS's Border and Transportation Security Directorate — to oversee several screening programs, including Secure Flight.[4]

Congress, meanwhile, included several provisions related to air passenger prescreening in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). Among other things, these provisions 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 utilizes the watch lists integrated and consolidated in the Terrorist Screening Database (TSDB);[5] (2) DHS to prescreen passengers on international flights against the TSDB prior to departure; and (3) TSA and DHS to establish appeals procedures by which persons who are identified as security threats based on records in the TSDB may appeal such determinations and have such records, if warranted, modified to alleviate such occurrences in the future.

Also, in the FY2005 DHS Appropriations Act (P.L. 108-334), Congress prohibited spending any funding provided under that act for the implementation, except on a test basis, of CAPPS II, Secure Flight, or any follow on/successor system, until the Government Accountability Office (GAO) reports that certain conditions have been met, including the establishment of an appeals process. GAO is expected

---

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

[4]Sara Kehaulani Goo, "Proposed Budget Would Strip TSA of Its Biggest Programs," *Washington Post*, Feb. 9, 2005, p. A06.

[5]The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) refers to the "consolidated and integrated terrorist watch list maintained by the Federal Government," which generally describes the TSDB maintained by the TSC.

to issue a report on the status of the Secure Flight (CAPPS II) program on March 28, 2005.[6]

Background on Civil Aviation Passenger Prescreening

Aircraft bombings[7] prompted the U.S. government to adopt a classified civil aviation passenger "No Fly" watch list in 1990, which was initially administered by the FBI. In late 1996, the FAA funded and oversaw the development of the CAPS system. In 1999, the FAA mandated that all major domestic and international U.S. carriers maintain and screen passengers with this system. Both the "No Fly" watch list and CAPS generally reside on the computer reservation systems used by U.S. air carriers; however, smaller airlines apparently still use paper lists. Following the 9/11 terrorist attacks, TSA began developing a next generation air passenger prescreening system known as CAPPS II, which generated considerable controversy.

"No Fly" and "Automatic Selectee" Watch Lists

The "No Fly" watch list is a list of persons who were considered to be a direct threat to U.S. civil aviation. It was administered by the FBI until November 2001, when it was then transferred to the FAA. The TSA later assumed administrative responsibility for the list, which was split into the "No Fly" and "Automatic Selectee" lists. The TSA places persons on these lists based on requests by the Department of Homeland Security and other members of the Intelligence Community.[8] The TSA distributes these watch lists to the U.S. air carriers. In turn, the air carriers screen passengers against these watch lists before boarding. In general, these watch lists are downloaded into a handful of computer reservation systems used by most U.S. air carriers.[9] As the names of these lists imply, passengers found to be on the "No Fly" list are to be denied boarding and referred to law enforcement, while those on the "Automatic Selectee" list are selected for secondary security screening before being cleared to board.

As intelligence and law enforcement officials were concerned about the security of the "No Fly" list, only a handful of names were on the list prior to the 9/11 attacks

---

[6]Chris Strohm, "DHS Budget Puts Administration on Collision Course with Lawmakers, Airlines," *Government Executive, Daily Briefing*, Feb. 9, 2005, go to [http://www.govexec.com/dailyfed/0205/020905c1.htm].

[7]The bombing of Pan Am 103 over Lockerbie, Scotland, Dec. 21, 1988 was a decisive event that prompted FAA officials to explore new options with which to increase U.S. aviation security.

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

[9]Ibid.

(less than 20).[10] Since then, the lists reportedly have been expanded almost daily.[11] According to one press account, there are more than 20,000 names on the "No Fly" list today, and TSA has been contacted by air carriers as many as 30 times per day with potential name matches in the recent past.[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 — Senator Edward Kennedy, and Representatives John Lewis and Don Young.[13] In other cases, misidentifications on international flights have led to costly diversions when air carriers have been prevented from entering U.S. airspace or continuing to their destinations. Despite problems that accompanied the expansion of the TSA "No Fly" list, the 9/11 Commission recommended that the "No-Fly" and "Automatic Selectee" lists be improved without delay.

Congress recently included provisions in the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) that require the Secretary of Homeland Security to establish a process by which persons could challenge the inclusion of their name on either the "No Fly" or "Automatic Selectee" lists, and have their names removed if warranted.[14] Another provision requires the "Security Privacy Officer" of the DHS to submit a report to certain congressional committees, within 180 days of enactment (June 15, 2005), assessing the efficacy of the "No Fly" and "Automatic Selectee" lists, including the impact of the use of these lists on privacy and civil liberties, and the ability of the Unites States to protect itself from terrorist attacks.[15]

Other U.S. Government Terrorist Watch Lists

In addition to improving the "No Fly" and "Automatic Selectee" lists, the 9/11 Commission recommended that air passengers be prescreened against the larger set of terrorist watch lists maintained by the U.S. government, which have been consolidated in a Terrorist Screening Database (TSDB) at the FBI-administered Terrorist Screening Center (TSC). Prior to 9/11, domestic air passengers were not screened against any other terrorist watch lists maintained by the federal government,

---

[10]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].

[11]Electronic Privacy Information Center, *Documents Show Errors*.

[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.

[14]Section 4012(a) of P.L. 108-458.

[15]Section 4012(b) of P.L. 108-458.

other than the "No Fly" and "Automatic Selectee" lists. Reportedly this continued to be the case as recently as September 2004.[16]

At the time of the 9/11 terrorist attacks, the U.S. government's principal terrorist watch list known as TIPOFF was maintained by the Department of State.[17] TIPOFF was the foundation of the TSDB.[18] At the time the TSC was established in Fall 2003, TIPOFF included over 120,000 records on terrorists and other criminals, including 81,000 distinct individual terrorist names.[19] As of October 2004, the TSC had downloaded over 102,000 terrorist "lookout" records in the FBI's National Crime Information Center (NCIC),[20] as compared to the approximately 20,000 names on the "No Fly" and "Automatic Selectee" lists.[21]

Also according to the FBI, the "No Fly" and "Automatic Selectee" lists were consolidated in the TSDB sometime in the latter half of FY2004.[22] It is unknown, however, whether domestic air passengers are being screened against the entire TSDB.[23] As not all known and suspected terrorists would be considered "threats to civil aviation," there could likely be legal and investigative policy considerations that would bear upon including all such persons who are known and suspected terrorists on the "No Fly" list and possibly the "Automatic Selectee" list. For example, the TSC may be reluctant to release the full list of known and suspected terrorists to the airlines due to data security concerns.

Meanwhile, in the Intelligence Reform and Terrorism Prevention Act of 2005 (P.L. 108-458), Congress 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 180 days of enactment (June 15, 2005) on the criteria for placing individuals in the integrated and consolidated TSDB watch lists 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 if listed persons are encountered.[24]

---

[16]Leslie Miller, "How Airlines, Government Check Watch Lists," *Associated Press*, Sept. 24, 2004.

[17]Briefing with Department of State's Bureau of Consular Affairs, Oct. 23, 2003.

[18]Ibid.

[19]Ibid.

[20]Briefing with the FBI Criminal Justice Information Services Division, Oct. 15, 2003.

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

[22]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, Oct. 2004, pp. 1-2.

[23]For further information, see CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by William J. Krouse.

[24]Section 4012(c) of P.L. 108-458.

Computer-Assisted Aviation Prescreening System (CAPS)

The CAPS system was developed following a known aircraft bombing and other suspicious incidents. The 1996 Federal Aviation Reauthorization Act authorized the development of the CAPS system.[25] The FAA, together with Northwest Airlines, developed the CAPS system in 1996 and 1997. Additional field testing continued through 1997 and 1998. The FAA issued a proposed rule directing all major U.S. air carriers to maintain CAPS on their computer reservation systems in April 1999.[26]

The operational concept behind the CAPS system is to select "high-risk" travelers based on certain characteristics found in Passenger Name Record (PNR) data elements — like ticket purchasing patterns and the details of their travel itineraries — for greater scrutiny in terms of baggage screening, while expediting baggage screening for "low-risk"passengers. In other words, the CAPS system was designed to determine which passengers were unlikely to have an explosive device in their checked baggage, so that limited explosive detection capabilities could be focused on a smaller number of passengers and bags.[27] The CAPS system was reviewed by the Department of Justice's Civil Rights and Criminal Divisions, along with the FBI, and was found not to be based on characteristics related to ethnicity, gender, or religious faith.[28] More recently, the CAPS system was renamed CAPPS (Computer-Assisted Passenger Presceening System).

The CAPPS system is largely invisible to the public, and the federal government does not control or collect data utilized by CAPPS, as the system itself resides on airline reservations systems (for example, Sabre and Amadeus).[29] While nine of the 19 hijackers were selected by CAPPS for additional *baggage* screening, it is significant that, on September 11, 2001, CAPPS was not used to select *passengers* for greater screening at passenger checkpoints.[30] While checkpoint screening was the principal measure to prevent aircraft hijackings, none of the 19 hijackers was prevented from boarding an aircraft following passenger checkpoint

---

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

[26]*Federal Register*, vol. 64, no. 74, Apr. 19, 1999, pp. 19219-19240.

[27]Statement of Jane Garvey to the National Commission on Terrorist Attacks Upon the United States, May 22, 2003, p. 11. Available at [http://www.9-11commission.gov/hearings/hearing7/witness_garvey.htm].

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

[29]Ibid., p. 200.

[30]Statement of Cathal L. Flynn to the National Commission on Terrorist Attacks Upon the United States, Jan. 27, 2004, p. 4. Available at [http://www.9-11commission.gov/hearings/hearing7/witness_flynn.htm].

screening.[31] Since 9/11, CAPPS has been expanded, and the system is also used by TSA to identify persons based on certain characteristics gleaned from the PNRs who are selected for not only greater passenger-checked baggage screening, but greater passenger checkpoint screening as well.

Computer-Assisted Passenger Prescreening System II (CAPPS II)

According to TSA, Secure Flight (see below) was developed after a lengthy review of the proposed and controversial next-generation domestic passenger screening system known as CAPPS II.[32] CAPPS II system was designed to use sophisticated algorithms to search both government and commercial databases to acquire limited background information on ticket-buyers to authenticate their identity. The system would have assigned travelers a color-coded categorical risk assessment as follows:

- Green-coded passengers would not have been considered a risk and would only have been subject to basic screening procedures — metal detectors and baggage x-rays.
- Yellow-coded passengers would have been deemed either an unknown or possible risk, and would have been subject to extra screening procedures — bag and body searches.
- Red-coded passengers would have been considered high risk and would not have been allowed to travel, and law enforcement officials would have been notified of their attempts to board commercial aircraft.[33]

In developing CAPPS II, TSA estimated that the total number of passengers flagged by the system would be reduced from the current rate of about 15% under existing CAPPS protocols, to about 5%.[34] Nevertheless, critics 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 by a corresponding increase in security.[35] Some legal scholars also questioned whether it would be permissible to prevent a person from boarding an aircraft on a mere suspicion of organizational affiliation.[36]

---

[31]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, pp. 6-7, available at [http://www.9-11commission.gov/staff_statements/staff_statement_3.pdf].

[32]Briefing with Department of State's Bureau of Consular Affairs, Oct. 23, 2003.

[33]*Federal Register*, Aug. 1, 2003, p. 45266.

[34]Sara Kehaulani Goo, "U.S. to Push Airlines for Passenger Records," *The Washington Post*, Jan. 12, 2004, p. A1.

[35]Jill D. Rhodes, "CAPPS II: Red Light, Green Light, or 'Mother, May I?,'" *The Homeland Security Journal*, Mar. 2004, p. 1.

[36]Ibid., p. 7. Also, see CRS Report RL32664, *Interstate Travel: Constitutional Challenges to the Identification Requirement and Other Transportation Security Regulations*, by Todd

(continued...)

In the FY2004 DHS Appropriations Act,[37] Congress prohibited the expenditure of any funding provided under that act, or any prior appropriations, to deploy or implement this new system until it had been evaluated by GAO. Furthermore, Congress required TSA to more adequately address eight action items before the CAPPS II system could be deployed in any manner except testing of the system. Congress placed similar prohibitions, action items, and GAO reporting requirements in the Vision 100 — Century of Aviation Reauthorization Act.[38] TSA indicated that it would continue to work closely with GAO, which was charged with certifying the adequacy of actions taken, to ensure that these requirements are met. The specific actions required by Congress include:

- establishing an internal oversight board;
- assessing accuracy of databases;
- stress-testing the system and demonstrating efficacy and accuracy;
- installing operational safeguards to protect the system from abuse;
- installing security measures to protect the system from unauthorized access;
- establishing policies for and effective oversight of system use and operation;
- addressing all privacy concerns; and
- creating a redress process for passengers to correct erroneous information.[39]

In February 2004, GAO found that TSA had only completed one of these eight action items: TSA had satisfactorily created an internal oversight board.[40]

GAO also reported that the development of this system was behind schedule, and TSA encountered major impediments in testing CAPPS II. In particular, the European Union and commercial airlines had been reluctant to hand over crucial data because of privacy concerns. Moreover, GAO underscored that CAPPS II, as designed, would be vulnerable to terrorists who assumed (i.e., stole or borrowed) another person's identity.[41] TSA anticipated that CAPPS II would have been integrated with US-VISIT, DHS's newly developed automated entry/exit control program.[42] Such a measure would have introduced a biometric component into the CAPPS II process for non-citizens, so that their identities could be confirmed with greater certainty.

In July 2004, the then acting TSA Administrator, David M. Stone, testified before the Senate Governmental Affairs Committee that CAPPS II was being

---

[36](...continued)
B. Tatelman.

[37]P.L. 108-90, 117 Stat. 1137.

[38]P.L. 108-176, 117 Stat. 2568.

[39]Section 519 of P.L. 108-90, 117 Stat. 1155.

[40]U.S. Government Accountability Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-040–385, (Feb. 2004), p. 4.

[41]Ibid., p. 4.

[42]*Federal Register*, Aug. 1, 2003, p. 45266.

"reshaped and repackaged" to address privacy issues.[43] The reshaped and repackaged system he spoke of is Secure Flight. In the FY2005 DHS Appropriations Act,[44] Congress prohibited the spending of any funds provided under that act for the deployment or implementation, other than on a test basis, of CAPPS II, Secure Flight, or other follow on/successor programs. In this act, Congress also revised the action items and required GAO to report back to the House and Senate Appropriations Committees by March 28, 2005.[45]

Secure Flight Test Program

TSA is developing the Secure Flight program — the next generation domestic passenger prescreening system — under the authority provided by the Aviation and Transportation Security Act.[46] According to TSA, Secure Flight consists of four elements: (1) a streamlined rule for more intensive screening; (2) a scaled-back identity authentication process; (3) a passenger name check against the Terrorist Screening Database; and (4) an appeals process for passengers who may have been misidentified. Hence, in addition to the appeals process, the Secure Flight test program is an amalgam of features taken from CAPPS, CAPPS II, and the 9/11 Commission's recommendation that passengers be screened against the wider set of terrorist watch lists maintained by the U.S. government. Within TSA, the Office of National Risk Assessment has responsibility for establishing policy for the Secure Flight program.

Streamlined Rule for Automatic Screening

Under the Secure Flight test program, TSA intends to assume the role of conducting behavioral-based prescreening that airlines now perform under the existing CAPPS system. The test-program, however, will use revised rules for selecting passengers for additional screening, which have been designed to reduce the number of passengers selected for secondary screening. Presumably, the specific factors considered will be continually reviewed and updated in light of changing threat evaluations and additional intelligence. A factor such as purchase of one-way tickets has probably lost any predictive value by now — if only because its inclusion in the program is widely known. In general, such a system must evolve as the potential strategies of terrorists evolve. In addition, TSA noted that some individuals will still be randomly selected for secondary screening to prevent terrorists from learning (through reverse engineering) the specific criteria used to select individuals under the Secure Flight program.

---

[43]Matthew L. Wald, "U.S. 'Reshaping' Airport Screening System," *New York Times*, (July 16, 2004), Section A, p. 18.

[44]P.L. 108-334, 118 Stat. 1319.

[45]Section 522 of P.L. 108-334, 118 Stat. 1320.

[46]P.L. 107-71, 115 Stat. 597.

Identity Authentication (IDA)

The test program apparently will also access limited commercial data to verify an individual's identity — a core concept of the CAPPS II proposed system. According to the Administration, this data will be evaluated separately and on a limited basis to determine whether such data can help to verify more accurately passenger identity during the pre-screening process.[47] In the original CAPPS II program, TSA had envisioned the use of commercial databases to authenticate the identity of a passenger before that passenger's information was compared against government-maintained terrorist and criminal databases. TSA has indicated that the IDA procedures would only be incorporated into the Secure Flight system if the following conditions are met:

- such measures do not result in inappropriate differential treatment of any category of persons;
- robust data security safeguards and privacy protections can be put in place to prevent unauthorized access to personal information; and
- the system enhances security and does not involve the U.S. government in storing or accessing commercial data but, rather, relies on commercial data aggregators to provide IDA services to the TSA.[48]

TSA has indicated that it will strive to meet the remaining requirements for CAPPS II implementation in the Secure Flight program, as the agency plans to establish a redress process for individuals who believe they have been unfairly or incorrectly singled out for additional screening or experience difficulties obtaining boarding passes.

Watch List Checks

As recommended by the 9/11 Commission, as part of Secure Flight, TSA will perform passenger name checks against the TSDB, which is maintained by the FBI-administered Terrorist Screening Center (TSC). According to the FBI, the "No Fly" and "Automatic Selectee" lists have been consolidated into the TSDB.[49] Due to this consolidation, it is likely that checks of these lists may be part of the more comprehensive TSDB check under the Secure Flight program. As part of this consolidation, it also is plausible that the TSC has assisted TSA in improving the "No Fly" and "Automatic Selectee" lists by cross-referencing terrorist records on those lists with other watch list records contained in the TSDB.

TSA will only prescreen domestic flights under Secure Flight, as CBP has assumed responsibility for prescreening passengers on inbound and outbound international flights. The TSC is assisting CBP — through the latter's National

---

[47]Briefing with Department of State's Bureau of Consular Affairs, Oct. 23, 2003.

[48]*Federal Register*, Sept. 24, 2004, p. 57353.

[49]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, Oct. 2004, pp. 1-2.

Targeting Center — with screening international air passengers against the TSDB. Air passengers on international flights are screened against the wider set of U.S. government terrorist watch lists through CBP's Advanced Passenger Information System (APIS), which is part of the Interborder Agency Inspection System (IBIS). It is unclear, however, as to the level of assistance the TSC is providing TSA with the day-to-day screening of domestic air passengers, including confirming possible matches. In addition, it is unclear whether the Administration's proposed Office of SCO — to be established under DHS's Border and Transportation Security Directorate — will be an effective mechanism to oversee multiple and varied screening programs.

Under agreement with the European Union, CBP will be provided with data from 34 specific categories of PNR data for travelers on international flights from EU countries.[50] Currently, a lesser amount of PNR data is transferred to APIS several times as it becomes available to the airlines on their reservation systems; however, final PNR data are sometimes not transferred to APIS until after the flight has departed (wheels up). In several recent cases, known or suspected terrorists have been allowed to board aircraft at airports abroad; and, subsequently, those flights were diverted or turned back.[51] As described earlier in the report, these cases have generated significant press coverage. To remedy these difficulties, the Intelligence Reform and Terrorist Prevention Act (P.L. 108-458) requires prescreening to be conducted prior to departure.

As part of Secure Flight, PNR data will be transmitted by the U.S. air carriers to TSA. These categories include specific ticketing and itinerary information, airfare data, frequent flier information, form of payment information, special service requests, among other things. They do not, however, include birth date information, which is not routinely collected by airlines. Birth date information was considered by TSA during the development of CAPPS II as an important data element for authenticating an individual's identity by comparing personal data provided by the passenger against records contained in commercial databases that are often used for conducting credit checks.[52]

Proposed TSA Passenger Advocacy and Redress Policy

The final element of the Secure Flight program includes the establishment of an Office of Identification Protection headed by a passenger advocate to provide an appeals process for possibly misidentified passengers. This new office would be separate from the TSA Ombudsman and Office of Privacy. As described above, as

---

[50]Bill Strassberger, *U.S. Federal News*, "DHS, EU Sign Agreement to Allow Collection of Passenger Data," May 28, 2004.

[51]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.

[52]Such commercial databases are maintained by private data providers like Acxiom and ChoicePoint, among others. For further information, see Robert O'Harrow, Jr., *No Place to Hide*, (New York, 2005), pp. 214-246.

part of the Secure Flight program, TSA will take over checking passengers names against terrorist watch lists, employ a streamlined rule to select certain passengers for closer examination, and tap commercial data providers to authenticate passenger identities. Through this Office of Identification Protection, TSA intends to provide redress to passengers who are possibly misidentified as terrorists, or inordinately selected for additional screening. According to TSA, the use of IDA will expedite the resolution of possible misidentifications.

In terms of simple misidentification, the passenger advocate would likely be able to clear such cases very quickly. Under current practice, persons who feel they have been misidentified are directed to contact the TSA Ombudsman, and they are often issued a "cleared" letter.[53] However, in cases where TSA believes a person is a suspected or known terrorist who poses a threat to civil aviation, challenges to such determinations would likely be much more complicated. The American Civil Liberties Union (ACLU) and privacy advocates have been critical of TSA's passenger advocacy proposal, because they maintain that such appeals should be handled by an adjudicative body that is independent of TSA.[54]

Border and Transportation Security Screening Coordination

The 9/11 Commission concluded that the U.S. intelligence and law enforcement community missed several vital opportunities to watch-list and screen several conspirators involved in the 9/11 terrorist attacks.[55] In addition, the Commission recommended that U.S. border and transportation security systems be integrated with other systems to expand the network of screening points to include the nation's transportation system and access to vital facilities.[56] To this end, the President issued Homeland Security Presidential Directive 11 (HSPD-11) on August 27, 2004.[57] Among other things, HSPD-11 called for enhanced and coordinated terrorist screening, while safeguarding civil liberties and privacy.

In its FY2006 budget request, the Administration has proposed creating an Office of Screening Coordination and Operations (SCO) within DHS's Border and

---

[53]The TSA Office of Ombudsman can be contacted at (571) 227-2383 or Omubudsman@dhs.gov.

[54]Caitlan Harrington, "TSA Promises New Advocacy Office to Clear Errors on No-Fly Lists," *CQ Homeland Security — Border Security*, Oct. 26, 2004.

[55]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.

[56]National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, p. 387.

[57]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].

Transportation Security Directorate.[58] The SCO mission would be to improve and coordinate programs aimed at detecting, tracking, and interdicting people, cargo, and conveyances that constitute a threat to the homeland; while, at the same time, facilitating legitimate travel and commerce. Within the SCO, the Administration proposes consolidating the following programs:

- United States-Visitor and Immigration Status Indicator Technology (US-VISIT),
- Secure Flight (formerly known as CAPPS II) and Crew Vetting,
- Free and Secure Trade (FAST driver registration only),
- Nexus/Sentri,
- Credentialing Administration and Operations,
- Transportation Worker Identification Credentialing (TWIC),
- Registered Traveler Program,
- Hazardous Materials Trucker Background Checks, and
- Non-citizen flight school checks.[59]

The Administration maintains that consolidating these programs under this office will promote common approaches and standards, and result in increased efficiencies and reduced redundancies. While the Administration's budget request suggests that the SCO will be responsible for the entire program budgets and system designs, it is unclear what control the office will have over the screening and credentialing activities of the TSA or CBP. Nevertheless, the Administration has indicated that the Secure Flight program will work "hand-in-hand" with CBP to integrate systems and provide "consistent and uniformly effective" domestic and international passenger prescreening.[60]

Key Operational Considerations

As described above, the Administration has adopted four approaches to air passenger prescreening as part of the Secure Flight program. These approaches, or systems, include (1) profiling passengers for more intensive searches of their persons and baggage, (2) identity authentication, (3) checks against the consolidated terrorist watch lists (TSDB), and (4) an appeals process for possibly misidentified passengers. Under these systems, criteria or rules will probably be developed to determine what constitutes a terrorist watch list hit, what passenger profiles trigger more intensive examinations of persons and baggage, or the amounts and types of data that can be gleaned from commercial data providers to authenticate a person's identity. The more robust the intelligence and the greater accuracy with which such rules are crafted, the more successful these systems will be.

---

[58]U.S. Department of Homeland Security, Fiscal Year 2006 Congressional Justification, Office of SCO, (Washington, Feb. 2005), p. SCO-2.

[59]Ibid., p. SCO-2.

[60]Ibid., p. SCO-9.

Type I and Type II Error Tradeoffs

In any screening system, including Secure Flight, there are essentially two classes of errors that can be made. The first class of errors, termed Type I errors or *false positives*, occur when a system erroneously signals a match. Such an error would occur when someone with no affiliation to terrorists is flagged by the system and either subjected to additional screening measures, detained, and/or denied aircraft boarding. In other words, a Type I error would occur anytime someone is misidentified by the system when the individual, in fact, poses no threat to aviation security. The second class of errors, termed Type II errors or *false negatives*, occur when the system fails to detect or identify that which the system has been designed to look for. In the case of Secure Flight, such an error would occur if a known or suspected terrorist or someone posing a threat to aviation were not identified by the system and boarded a flight without additional scrutiny. The costs and benefits of the Secure Flight program are shaped by the following three factors.

False Negatives. First, Type II errors (false negatives) are potentially much more costly than Type I errors (false positives). Although difficult to quantify, the potential costs associated with just one Type II error may far outweigh the costs of more frequent Type I errors. If another major catastrophe — like the terrorist attacks of September 11, 2001 or the bombing of Pan Am flight 103 over Lockerbie, Scotland in December 1988 — were to occur, the chain of failures in security leading up to such events, including the possible failure to detect terrorists during prescreening, could result in many lives lost, multi-billion dollar direct costs, and lasting economic impacts to the aviation industry. Reducing Type II errors will be dependent upon the quality, quantity, and timeliness of the intelligence (terrorist identities) produced by the U.S. Intelligence Community and law enforcement as well as issues like system integrity and the accuracy of data entry.

False Positives. Second, Type I errors (false positives) are likely to be much more frequent than Type II errors. While there are greater than 600 million passenger boardings on commercial aircraft each year,[61] the consolidated terrorist screening database includes only about 100,000 individual identities.[62] Moreover, many of these known and suspected terrorists probably live and operate outside the United States, decreasing the likelihood that they would be encountered on a domestic flight.[63] Nevertheless, even if a small percentage (less than 1%) of passengers were flagged (e.g., for having a name similar to a listed name), this would likely generate thousands of false positives each year.

---

[61]U.S. Department of Transportation, Federal Aviation Administration, Office of Aviation Policy & Plans, *FAA Aerospace Forecasts, Fiscal Years 2004-2015*, Mar. 2004.

[62]Eric Lichtblau, "To Streamline its Response, U.S. Creates a Terror 'Watch List,'" *International Herald Tribune*, Sept. 18, 2003.

[63] In 2002, it was estimated that only about 5,000 individuals associated with al Qaeda were operating in the United States. See Bill Gertz, "5,000 in U.S. Suspected of Ties to al Qaeda," *The Washington Times*, July 11, 2002.

The implications of Type I errors based principally on name-based checks of the "No Fly" list or the consolidated TSDB are that such persons would possibly be detained or prevented from boarding an aircraft. Furthermore, a passenger profiling system that selects an inordinate number of persons for more intensive examinations would not only inconvenience flagged passengers, but would likely slow the screening process and consume scarce resources at unacceptable rates. On the other hand, if system designers were able to craft an effective means for assessing passenger risk, then, it could be possible to focus limited screening resources more efficiently on a smaller number of "high-risk" persons. In regard to proposed procedures under Secure Flight to authenticate a person's identity, these methods are untested. Such procedures, however, could plausibly be used to alleviate misidentifications of persons whose names were similar to those on the "No Fly" list or in the consolidated Terrorist Screening Database.

Limits of Intelligence. The third factor regarding the Secure Flight program is that little is known publically about the limitations of the intelligence/data and rules that are, or will be, used by screening agencies to identify known or suspected terrorists, or to select persons who fit a particular profile for more intensive examinations. Regardless, it is possible that adjusting the screening system to reduce the probability of one of these types of errors will increase the probability of the other type. Hence, designing prescreening criteria for identifying terrorists or selecting passengers for greater examination of their persons or baggage involves a balancing act between the two types of errors. For the near future, screening agencies will probably err on the side of caution. As one expert surmised, in the current context of heightened aviation security in the aftermath of September 11, 2001, "... [T]he growth in danger from Type II errors necessitates altering our tolerance for Type I errors. More fundamentally, our goal should be to minimize both sorts of errors."[64] Unavoidably, though, tradeoffs must be made in setting operational criteria for the system.

Congressional Requirements. In the FY2005 DHS Appropriations Act,[65] Congress directed the GAO to report to Congress on whether the Secure Flight program and its underlying processes to authenticate a passenger's identity or assign risk scores will produce a large number of false positives (misidentifications) or an inefficient diversion of security resources. Also, in the Intelligence Reform and Terrorism Prevention Act of 2004, Congress required that the federal databases used to establish a person's identity under the Advanced Airline Passenger Prescreening system not produce a large number of false positives.[66] (See **Appendix I**.)

Balancing Benefits and Risks. TSA will have to weigh potential benefits and risks in developing the Secure Flight program. Benefits could include

---

[64]Testimony of Paul Rosenzweig, Senior Legal Research Fellow, Center for Legal and Judicial Studies, The Heritage Foundation Before the U.S. House of Representatives, Committee on Transportation and Infrastructure, Subcommittee on Aviation Regarding the Transportation Security Administration's CAPPS II. Mar. 17, 2004.

[65]Section 522 of P.L. 108-334, 118 Stat. 1319.

[66]Section 4012(a) amends 49 U.S.C. 44903(j)(2) — with a new Subparagraph (C).

preventing known or suspected terrorists from boarding commercial aircraft by focusing limited passenger screening resources on individuals 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. Risks could include potentially compromising personal data and singling out certain passengers unfairly, because of a lack of accurate terrorist identities and threat data, or other system limitations. The balancing of risks and benefits in the Secure Flight system can be framed in terms of the tradeoffs between falsely flagging passengers by the system on the one hand, and failing to detect a terrorist before boarding on the other hand. Hence, finding a balance between the two competing objectives of minimizing misidentifications, while effectively detecting terrorists is central to the design of Secure Flight.

Redress and Remedy

As described earlier in this report, when the FAA and TSA expanded the use of the "No Fly" and "Automatic Selectee" lists following the 9/11 terrorist attacks, an increasing number of highly visible and high-profile misidentifications were the result. It is notable that the TSA did not have adequate manpower to respond directly to possible matches, since they did not have a large presence across the country. Also, the FBI had redirected significant resources to ongoing counterterrorism investigations. Consequently, many misidentifications were not resolved in a timely manner. Furthermore, there was no formal process by which corrective action could be taken to alleviate or prevent future misidentifications.

Watch List Consolidation at FBI-Administered TSC. At some point in FY2004, "No Fly" and "Automatic Selectee" list checks were integrated (fused) with the ongoing terrorist screening operations of the FBI-administered TSC. In large part, this fusion was likely prompted by press accounts that persons on "terrorist watch lists" had been allowed to board international flights to the United States. Some of these flights were held on the tarmacs of international airports abroad, as part of a larger investigation to disrupt an al Qaeda conspiracy to attack U.S. targets with airliners.[67] Other flights, including the flight carrying pop star Cat Stevens (Yusuf Islam), were diverted to Bangor, Maine.[68] In a more recent case, a British Airways flight returned to Heathrow Airport in London, England, and an unidentified passenger was taken into custody after his name matched that of a suspected member of a Moroccan terrorist group.[69]

---

[67]In Dec. 2003, 10 US-bound flights were grounded abroad (two British, six French, and two Mexican), after intelligence emerged that al Qaeda intended to hijack several commercial flights and use them in a suicide attack against U.S. targets, following checks of U.S. terrorist watch lists. See David Leppard, "Terror Plot To Attack US with BA Jets," *Sunday Times* (London), Jan. 4, 2004, p. 1.

[68]Sara Kehaulani Goo, "Cat Stevens Held After D.C. Flight Diverted," *Washington Post*, Sept. 22, 2004, p. A10; and "U.S.-bound Air France Flight Diverted Due to Passenger," *Agence France Presse*, Nov. 21, 2004.

[69]Justin Rood, "As Ridge Warns of al Qaeda Determination, British Flight to the United States Turned Back," *CQ Homeland Security — Intelligence*, Jan. 12. 2005, and "U.S.-
(continued...)

Moreover, as part of the Secure Flight program, the Administration announced that CBP would assume responsibility for screening international flights, while the TSA would continue to be responsible for domestic flights. In any case, whether on international or domestic flights, watch list checks and the resolution of possible matches were, and have been, assumed by the TSC in coordination with the CBP and the TSA.

Which Agency Will Handle Passenger Appeals: TSA, TSC, or Other? As part of Secure Flight, TSA has shouldered the responsibility for processing complaints about possible and continuing misidentifications. In addition, a class action suit has been filed by the ACLU concerning the administration of the "No Fly" list by TSA.[70] Previously, however, the TSC Director had been made responsible for developing policies and procedures related to criteria for inclusion into the consolidated TSDB; and measures to be taken in regard to misidentifications, erroneous entries, outdated data, and privacy concerns. At the same time, the Administration maintains that since the TSC does not collect intelligence, and has no authority to do so, that all intelligence or data entered into the TSDB has been collected in accordance with the preexisting authorities of the collecting agencies. The same could be said for TSA, however. Hence, questions could arise as to whether TSA is in any better position than TSC to handle matters pertaining to passenger redress. The issue of redress may be further complicated by the proposed creation of the SCO. If not properly coordinated, inconvenienced passengers could face a bureaucratic maze when seeking redress.

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.[71] Also, Members have asked how a person would find out if they were in the Terrorist Screening Database, and if so, how did they get 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 also suggested that the TSC would probably be unable to confirm or deny whether the person was in the TSDB under current law.[72]

---

[69](...continued)
bound British Jet Returns to London After US Refuses to Admit Passenger," *Agence France Press*, Jan. 12, 2005.

[70]American Civil Liberties Union, *ACLU Files First Nationwide Challenge to 'No-Fly' List, Saying Government List Violates Passengers' Rights*, Apr. 6, 2004, go to [http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15430&c=272].

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

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

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,[73] 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 watch list. However, under national security and law enforcement FOIA exemptions, the departments may withhold records on whether an individual is on a watch list.[74] 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[75] request with DHS and/or the Department of Justice to discern whether the TSA 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. While the Privacy Act generally does not restrict information-sharing related to known and suspected terrorists who are not U.S. persons for the purposes of visa issuance and border inspections, it does restrict the sharing of information on U.S. persons (citizens and legal permanent residents) for purely intelligence purposes, who *are not* the subject of on-going foreign intelligence or criminal investigations.[76] Consequently, legal questions concerning the inclusion of U.S. persons on various watch lists under criminal or national security predicates may arise. In addition, questions of compensation for persons mistakenly damaged by inclusion in these databases will likely be an issue.

Congressional Requirements. As noted earlier in the report, Congress included provisions in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) that require the TSA Assistant Secretary for Homeland Security to establish a timely and fair process for individuals identified as a threat as part of an advanced airline passenger prescreening process required to be established under the same Act. This process would compare passenger names against the "No Fly," "Automatic Selectee," and consolidated terrorist screening database prior to the

---

[73]5 U.S.C. §522.

[74]5 U.S.C. §§522(b), (c), 522a(j).

[75]5 U.S.C. §522a.

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

aircraft's departure. The provision requiring the establishment of this process also requires that the databases used to "verify the identity of passengers" not result in a large number of false positives.[77] (See **Appendix I**.)

Also, in the FY2005 DHS Appropriations Act,[78] Congress prohibited spending any funding provided under that act, or any prior appropriations, for the deployment or implementation, except on a test basis, of CAPPS II, Secure Flight, or any follow on/successor system, until GAO reported that an appeals process (a system of due process) had been established to allow air passengers either delayed or prohibited from boarding a flight to challenge TSA determinations that they posed a threat to civil aviation and correct false information about themselves.

Systems Integrity, Access, and Data Retention

Addressing database accuracy is likely to be an ongoing concern and directly involves the TSC and potentially the Terrorist Threat Integration Center (TTIC)[79] as well.[80] In essence, at each of these layers in the terrorist information collection, integration, and dissemination process, adequate quality assurance (QA) mechanisms will be needed to assure data integrity and accuracy. TSA and the Secure Flight system can, in large part, be viewed as an end user system or access portal to these terrorist data. While TSA will need to provide QA to ensure it accurately pulls data from these sources or pushes PNR data into these systems, QA of the TSDB and TSC systems will largely be the responsibility of the FBI, as the Bureau administers the TSC. Likewise, security and access controls and overarching policies regarding system use and oversight of system operations will likely involve extensive cooperation between the TSA and the FBI to establish appropriate data access protocols, data encryption, secure data transmission capabilities, among other subjects.

Data access and retention has been an ongoing concern regarding CAPPS II implementation and may well become an even greater concern under the proposed Secure Flight system since the TSA now proposes directly to receive and control the PNR data. Secure data transmission between air carriers and reservation systems on the one end, and the TSA on the other, is also likely to be an area of concern.

Systems Platform and Infrastructure

As discussed above, CAPPS currently runs on the computer reservation systems used by U.S. air carriers. If the Secure Flight program is adopted, it will

---

[77]Section 4012(a) amends 49 U.S.C. 44903(j)(2) — with a new Subparagraph (C).

[78]P.L. 108-334, 118 Stat. 1319.

[79]Under E.O. 13354 and P.L. 108-458, the TTIC has been incorporated into the National Counterterrorism Center (NCTC). Hence, it falls under the purview of the Director of National Intelligence.

[80]For further information on the linkages and interactions between the TSC and TTIC, see CRS Report RL32366, *Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6*, by William J. Krouse.

likely require TSA to establish a secure system and telecommunications network to take in the PNR data, process it at some central locale (or regional locales), and send the processed results back to the passenger and baggage screening checkpoints. TSA's prior work on CAPPS II development may provide a framework for secure data transfer, data access, and data retention. Nonetheless, costs and logistics for providing secure interactions with these private computer reservation systems containing PNR data may be a challenge in terms of policies and procedures as well as technologies to ensure security and integrity of the data.

Registered Traveler Pilot Program[81]

TSA has also launched the Registered Traveler Pilot Program to improve and streamline the screening process for pre-approved travelers. The program was extended through FY2006.[82] Program eligibility was initially limited to U.S. citizens, U.S. nationals, or legal permanent residents who have been identified by TSA as frequent fliers and invited to join the program. Program applicants undergo a security assessment that includes analysis of criminal history and intelligence databases. Approved program participants are positively identified at designated home airports through biometric technology, and their security screening is expedited through dedicated screening lanes. According to TSA, evaluations of the pilot program being tested at five airports will determine the future of this program. Those airports are Boston, Houston, Los Angeles, Minneapolis-St. Paul, and Washington, DC.

The TSA initially indicated that the Registered Traveler program would not be integrated into the Secure Flight program.[83] The Administration's FY2006 DHS budget request, however, included a proposal to create an Office of SCO that suggests these programs will be integrated at some level.[84] Also, in January 2005, DHS expanded the pilot program to include certain European Union travelers departing from Schiphol Airport in Amsterdam and arriving at John F. Kennedy Airport in New York City. For international travelers (U.S. citizens, legal permanent residents, or foreign visitors), this program will likely be integrated with CBP screening processes, including US-VISIT for non-US citizens. An issue for Congress will be the coordination between TSA and CBP, and possibly other agencies, in integrating pilot programs to expedite screening with routine screening processes like Secure Flight or US-VISIT.

---

[81]Department of Homeland Security, Transportation Security Administration, *What is Registered Traveler?* go to [http://www.tsa.gov/interweb/assetlibrary/Factsheet.pdf].

[82]Zack Phillips, "TSA Extends Registered Traveler Pilot Program Through September," *CQ Homeland Security — Transportation & Infrastructure*, Jan. 27, 2005.

[83]Justin Oberman, Director, Office of National Risk Assessment, Transportation Security Administration, "Secure Flight: Screening for Terrorists on Passenger Planes," presentation given at the Heritage Foundation on Oct. 21, 2004, available at [http://www.heritage.org/Press/Events/ev102104a.cfm].

[84]U.S. Department of Homeland Security, Fiscal Year 2006 Congressional Justification, Office of SCO, (Washington, Feb. 2005), p. SCO-2.

Prescreening in Other Transportation Modes

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) includes a provision that would require the DHS to implement a process for vetting the names of passengers and crew carried on cruise ships against the consolidated terrorist watch list. Again Secure Flight or a similar system may provide the capabilities to meet such a mandate. If a single system such as Secure Flight is to be used to meet these requirements, a key system design issue will be whether the system can handle the extensive and varied demands that will be placed on it by the aviation and cruise ship industries, and whether it can provide uninterrupted data access to meet these requirements. While not formally proposed, some may also consider whether it would be beneficial to expand prescreening practices into additional transportation modes such as passenger rail and intercity bus operations.

Avoiding "Mission Creep"

While proposing to expand prescreening beyond commercial airline travel may be viewed by some as a form of "mission creep" that could introduce significant system design challenges to meet these varied objectives, it is fundamentally different than the controversial "mission creep" that some critics of the CAPPS II development have warned against.[85] In the case of CAPPS II, there was significant concern that proposals to use that system for other law enforcement purposes, such as comparing names against available criminal information databases to evaluate the risk posed by a passenger,[86] would detract from the system's principal objective of identifying known or suspected terrorists that attempt to infiltrate the aviation system.[87]

These concerns focused on how doing so could overly burden the TSA and significantly expand its role, and how widespread inaccuracies in these criminal databases could create significant hassles for air travelers as well as for the TSA. Another form of "mission creep" rebuffed by critics was the concept of data mining commercially available information on a traveler to devise a tailored risk score for that individual which could then be used to determine the level of screening or scrutiny for that passenger.[88] Both of these concepts have been abandoned in the

---

[85]American Civil Liberties Union, *ACLU Comments to Department of Homeland Security on the 'Passenger and Aviation Security Screening Records,'* Sept. 30, 2003, available at [http://www.aclu.org/news/NewsPrint.cfm?ID=13847&c=206].

[86]While the plan for CAPPS II was expanded to consider checking PNR data against government-maintained criminal records, such as the NCIC database, the TSA has limited the scope of the Secure Flight program to focus solely on comparing PNR data to available data on suspected and known terrorists. According to the TSA, the system will not be used for other law enforcement purposes such as checking passengers for outstanding law enforcement "wants and warrants," or other "hot files" resident on the NCIC.

[87]Deborah Charles, "Critics Say U.S. Airlines Screening Plan Intrusive," *Washington Post*, Aug. 25, 2003.

[88]Joan M. Feldman, "Mission Creep," *Air Transport World*, May 2004, pp. 48-50.

development of the Secure Flight program, and TSA has indicated that its sole focus in Secure Flight is vetting passenger data against the consolidated watch list.[89]

Augmenting Prescreening with Behavioral-Based Evaluations

While the TSA has apparently abandoned integrating data mining and the use of non-terrorism-related databases such as criminal history databases in the architecture of Secure Flight, TSA is apparently still mulling concepts of how to integrate behavioral-based evaluations into the passenger prescreening process. Behavioral-based evaluations — examining factors such as ticket purchasing patterns or flight activity — are a core concept of the existing CAPPS program run by the airlines under their individual security programs. The TSA has indicated that it will refine and integrate these behavioral evaluation methods in Secure Flight and will also integrate a random selection process for additional screening, a recommended practice to ameliorate terrorists from reverse-engineering the system to determine what behavioral factors it considers.

It has also been reported that the TSA plans to train screeners to use observational techniques to single out individuals for additional scrutiny based on unusual or anxious behavior exhibited at screening checkpoints.[90] Screeners will be trained in the technique, known as Screening of Passengers by Observation Techniques (or SPOT) which is based on an ongoing program called the Behavior Assessment Screening System (or BASS) developed by the Massachusetts State Police for use at Boston Logan International Airport. This program is not a part of Secure Flight, but is being explored as an additional tool for assessing passenger risk characteristics. While this program implements a technique based on behavioral-based evaluations, it is likely that its implementation may become controversial and could generate additional oversight including of how the technique is applied and whether it differentially targets individuals from any particular racial, religious, or ethnic group.

Fitting into the Larger Strategy

Finally, in adjusting the decision criteria in Secure Flight, it must be remembered that the pre-screening step is just one element in a larger, multiple-layer security strategy. All passengers will go through some inspection of their person and luggage; the pre-screening step determines only which will be selected for more intense scrutiny (and the relatively few who will be denied boarding altogether). Thus, the cost of a Type II error — allowing a terrorist to board a passenger flight undetected — depends critically on the performance of the other layers in the aviation security system. If there is relatively high confidence that the screening process is capable of detecting and preventing the carriage of dangerous items (weapons, explosives, and other threat objects), and that in-flight security measures — such as

---

[89]U.S. Department of Homeland Security, Press Office, *TSA To Test New Passenger Pre-Screening System*, Aug. 26, 2004.

[90]Sally B. Donnell, "Spotting the Airline Terror Threat," *Time (Online Edition)*, Oct. 2, 2004. [http://www.time.com/time/nation/article/0,8599,708924,00.html].

air marshals, hardened cockpit doors, trained flight attendants and armed pilots — are believed to be effective, then the potential cost of failing to detect a terrorist in the prescreening process may be offset by these additional layers of security. If so, then it may be reasonable to establish somewhat more lenient criteria for selecting passengers for additional scrutiny, reducing the frequency and total cost of Type I errors. Still, despite the layered strategy, it would be prudent to keep in mind that, in the safety field, virtually all accidents in complex systems can be traced to multiple failures in redundant layers of safety.[91]

Possible Issues for Congress

As described above, certain steps taken by the Administration regarding the Secure Flight program, CBP prescreening of passengers on international flights, and the consolidation of the "No Fly" and "Automatic Selectee" lists in the consolidated terrorist screening database, have raised issues for Congress. In addition, Congress has included air passenger prescreening provisions in two recently enacted laws. These actions may generate the following oversight issues for Congress:

- To what extent has the screening of domestic air passengers by TSA, and international air passengers by CBP, been integrated with the operations of the TSC? In other words, has TSA's day-to-day administration of the "No Fly" and "Automatic Selectee" lists been adequately integrated with the TSC's operations? How has this integration benefitted the day-to-day operations of the TSA and the CBP?
- Have the terrorist name records on the "No Fly" and "Automatic Selectee" lists been adequately improved by cross-referencing, and possibly expanding, them with the records in the TSDB maintained by the FBI-administered TSC?
- If the TSA and CBP manage to negotiate the transfer of the final passenger manifests and name records from domestic and international airlines in a fashion that allows those agencies to complete a final TSDB check prior to departure (wheels up), will the watch list screening under Secure Flight be sufficient to meet the advanced airline passenger prescreening system required by the Intelligence Reform and Terrorism Prevention Act of 2004?
- In regard to shared jurisdictions, will it be possible to cleanly divide responsibility for screening air passengers on both arriving and departing domestic and international flights between TSA and CBP?
- How will the proposed creation of the SCO, at DHS' Border and Transportation Security Directorate, delineate the roles and responsibilities of the office, TSA, and CBP with regard to passenger prescreening?
- 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" lists from the airlines?
- What agency will be responsible for setting out the data elements needed for inclusion in the passenger name record to effectively screen known and

---

[91] James Reason, *Managing the Risks of Organizational Accidents* (Burlington, Vermont: Ashgate, 1997).

suspected terrorists, as well as others who may credibly present a known threat to civil aviation?
- Will such data elements be different for domestic flights as compared to international flights?
- In regard to the administration of the "No Fly" list by TSA, will it be possible for TSA to implement an appeals process that will provide adequate redress and remedy to those persons mistakenly identified as a "threat to civil aviation?" What impediments to redress exist? Multiple agencies? Restricted access to information?
- Will the Registered Traveler pilot program be integrated into the TSA Secure Flight program and the CBP international air passenger prescreening program?

Conclusion

In the current aviation security environment, some believe that a terrorist attack involving a civilian aircraft remains a grave concern. The adequacy of current security measures — including existing systems used to screen air passengers against terrorist watch lists — has been questioned, most recently by the 9/11 Commission. At the same time, considerable controversy surrounds existing air passenger prescreening systems, such as the TSA's "No Fly" list. Such controversy underscores that screening air passengers for more intensive searches of their persons or baggage, or to prevent them from boarding an aircraft in the event of a terrorist watch list hit, is likely to be a very difficult proposition for the federal agencies tasked with providing aviation security — namely the TSA, CBP, and the FBI-administered Terrorist Screening Center.

Despite the controversial nature of air passenger prescreening, most would agree that the federal government should prevent a person for whom there was sufficient intelligence available to the U.S. government (through its intelligence and law enforcement agencies) to consider them a suspected terrorist and a threat to civil aviation from boarding a commercial aircraft. Consequently, policy makers and system developers are tasked with designing a system that will be sufficiently sensitive to detect known and suspected terrorists (based in large part on timely and accurate intelligence) and specific enough not to misidentify others as terrorists. At the same time, only an extremely small percentage of air passengers will actually be terrorists. Hence, misidentifications (false positives) could be more frequent than desired. Moreover, misidentified persons could be sorely inconvenienced or, worse, possibly having their civil rights infringed upon. Such events could likely be highly visible to the public and could undermine public confidence in these aviation security measures.

If newly implemented screening systems should fail on either count — failing to detect terrorists or producing an unacceptably large number of misidentifications — public support for such aviation security systems may erode rapidly and severely undermine the public standing of agencies tasked with administering such systems. In other words, the tradeoff between the relatively low probability of encountering and detecting terrorists and the high probability of frequent misidentifications poses a persistent challenge to effectively implementing passenger prescreening.

In response to misidentifications based on the "No Fly" list, Congress has recently required the Department of Homeland Security to develop an appeals process for persons who are denied the ability to board a flight, because their names or names similar to theirs, were on that list. To some extent, a viable and comprehensive appeals process that provides redress and remedy to persons misidentified as terrorists may be one way to compensate for an inevitable level of misidentifications.

Appendix A. Related Provisions Included in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458)

While the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) does not include provisions that directly address the Terrorist Screening Center's mission of establishing a consolidated Terrorist Screening Database, the act includes several provisions that require the TSA to: (1) assume the airline passenger prescreening function from U.S. air carriers after it establishes an advanced passenger prescreening system for domestic flights that utilizes the watch lists integrated and consolidated in the TSDB;[92] (2) prescreen airport personnel against the TSDB prior to allowing them access to secure/operational airport areas; (3) prescreen persons seeking to lease or rent aircraft over 12,500 pounds (at the operator's request); (4) establish an appeals process by which persons who are identified as security threats based on TSDB watch lists may challenge such determinations to TSA and, if warranted, have such records modified to alleviate such occurrences in the future; (5) prescreen passengers on international flights against the TSDB prior to departure; (6) report to Congress on (a) the criteria used to place persons in the TSDB and (b) the privacy and civil liberty implications of the further use of the "No Fly" and "Automatic Selectee" lists; (7) prescreen foreign law enforcement officers against the TSDB prior to providing them with air marshal training; and (8) prescreen maritime vessel passengers.

Advanced Airline Passenger Prescreening System[93]

Section 4012(a) of P.L. 108-458 required the Transportation Security Administration Assistant Secretary for Homeland Security to begin testing by January 1, 2005 an advanced airline passenger prescreening system that will allow DHS to compare air passenger information against the "No Fly," "Automatic Selectee," and TSDB. Within 180 days of the successful testing of this system, DHS is required to assume the air passenger prescreening function from U.S. air carriers. The following system requirements are set out:

- establish a procedure for airline passengers, who are delayed or prohibited from boarding, because they were identified by the system as posing a security threat, to appeal such determinations and, if warranted, have the system's records modified to alleviate future delays and inconveniences;
- ensure that federal government databases used by the system to verify the identity of passengers will not result in large number of false positives;
- establish an internal oversight board to oversee and monitor the manner in which the system is being implemented;
- establish sufficient operational safeguards to reduce opportunities for abuse;
- implement substantial system security measures to prevent unauthorized access;

---

[92]The bill refers to the "consolidated and integrated terrorist watch list maintained by the Federal Government," which generally describes the TSDB maintained by the TSC.

[93]Section 4012(a) amends 49 U.S.C. 44903(j)(2) — with a new Subparagraph (C).

- adopt policies for effective oversight of the use and operation of the system; and
- ensure that there are no specific privacy concerns with the technological architecture of the system.

In addition, the TSA Assistant Secretary is authorized to require air carriers, and those providing booking services and systems to air carriers, to supply the necessary passenger information to begin implementing this system within 180 days of the completion of testing.

Prescreening of Airport Employees and Others[94]

Section 4012(a) requires the TSA Assistant Secretary, in coordination with the Secretary of Transportation and the FAA Administrator, to screen all persons allowed unescorted access to certain secure/operational areas of airports against the consolidated TSDB prior to being granted such access. In addition, the law requires that anyone seeking FAA certification (e.g., a pilot or mechanic's license) also be screened against the TSDB.

Chartered and Leased Aircraft Customer Prescreening[95]

Section 4012(a) requires the TSA Assistant Secretary to establish a process by which operators of charter and leased aircraft may request that persons seeking to lease or rent aircraft with a maximum takeoff weight of greater than 12,500 pounds be screened against the consolidated TSDB prior to being allowed access to such aircraft. If such persons are identified as posing a security threat following screening, then the operators are authorized to refuse service. In regard to such screening, the operating requirements set out for the airline passenger screening system (listed above) are applicable.

Also, under this provision, the Secretary for Homeland Security, in consultation with the Terrorist Screening Center, is required to develop guidelines and procedures for the collection, removal, and updating of data maintained in the "No Fly" and "Automatic Selectee" lists.

Appeal Procedures[96]

Section 4012(a) requires the TSA Assistant Secretary for Homeland Security to establish a timely and fair process for individuals identified as a threat under provisions described above — regarding airline passengers, airport access, or chartered and leased aircraft customers — to appeal such determinations and correct any erroneous information in those records (if warranted). The TSA Assistant Secretary is required further to maintain records on misidentified and delayed

---

[94]Section 4012(a) amends 49 U.S.C. 44903(j)(2) — with a new Subparagraph (D).

[95]Section 4012(a) amends 49 U.S.C. 44903(j)(2) — with a new Sbparagraph (E).

[96]Section 4012(a) amends 49 U.S.C. 44903(j)(2) — with a new Subparagraph (G).

persons, so that such records include corrected/updated information as well as information to authenticate their identity.

International Passenger Prescreening[97]

Section 4012(a) requires the Secretary for Homeland Security to issue proposed regulations that will allow the DHS to attain passenger information for all international flights and compare it to the consolidated TSDB prior to the flight's departure. It also requires that the Secretary establish a "timely and fair" process by which persons identified as a security threat based on information contained in the TSDB watch lists be allowed to appeal such determinations to DHS and to correct any erroneous information. As under the TSA advanced airline passenger prescreening system (for domestic flights), the Secretary for Homeland Security is required to maintain records on misidentified and delayed persons, so that such records include corrected information as well as information to authenticate their identity. For international flights, it is likely that CBP, in coordination with the TSC, would maintain such records as part of their responsibilities to screen international flights.

Report on Effects on Privacy and Civil Liberties

Section 4012(b) of P.L. 108-458 requires the Security Privacy Officer of the DHS to submit, within 180 days of enactment (June 15, 2005), a report assessing the impact of the "No Fly" and "Automatic Selectee" lists on privacy and civil liberties 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. It also requires that this report include recommendations to eliminate or minimize the adverse effects these watch lists may have on privacy, due process, and civil liberties, as well as on the possible application of these lists to other modes of transportation. Furthermore, it requires that the report include analysis on the extent to which the use of these lists may increase the ability of the Unites States to protect itself from terrorist attacks.

Report on Criteria for Inclusion in the Consolidated TSDB

Section 4012(c) of P.L. 108-458 requires 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 (June 15, 2005) on the criteria for placing individuals in the integrated and consolidated TSDB watch lists 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 if listed persons are encountered.

---

[97]Section 4012(a) amends 49 U.S.C. 44909(c) — with a new Paragraph (6).

Foreign Air Marshal Trainees Prescreening

Section 4018 requires that foreign law enforcement officers be screened against the TSDB before receiving air marshal training from DHS.

Maritime Vessel Passenger Prescreening

Section 4071 requires the Secretary of Homeland Security, within 180 days of enactment (June 15, 2005), to implement a procedure by which passengers and crew members on cruise ships embarking or disembarking passengers at U.S. ports of entry would be (1) compared with the TSDB to prevent known or suspected terrorists from boarding such vessels, and (2) selected for additional security screening through the use of "no transport" and "automatic selectee" lists. For passengers embarking at foreign ports of entry, this provision provides a waiver for the use of "no transport" and "automatic selectee" lists if the Secretary deems that use of such lists is impracticable. It would also authorize the Secretary to require the necessary information from cruise ship operators in order to comply with the above requirement.

Furthermore, this provision would require the Secretary of Homeland Security, in consultation with the FBI Director, to design guidelines, policies, and procedures regarding the maintenance of the watch list database to ensure accuracy and integrity. Section 4071 would also require the Secretary of Homeland Security to establish a simple and timely method for correcting erroneous entries and adding clarifying information to minimize or eliminate false hits and misidentifications.

Appendix B. Frequently Used Abbreviations

To aid the reader, the following list of abbreviations is provided.

APIS	Advanced Passenger Information System
CAPS	Computer-Assisted Aviation Prescreening System
CAPPS	Computer-Assisted Passenger Prescreening System
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
DOJ	Department of Justice
DOS	Department of State
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
HSPD-11	Homeland Security Presidential Directive 11
IBIS	Interagency Border Inspection System
NCTC	National Counterterrorism Center
NCIC	National Crime Information Center
NTC	National Targeting Center
PNR	Passenger Name Record
SCO	Office of Screening Coordination and Operations
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TTIC	Terrorism Threat Integration Center
U.S.-VISIT	U.S. Visitor and Immigrant Status Indicator Technology Program