Congressional Research Service
Informing the legislative debate since 1914

Risk-Based Approaches to Airline Passenger Screening

Bart Elias
Specialist in Aviation Policy

March 31, 2014

Congressional Research Service
7-5700
www.crs.gov
R43456

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Until recently, the Transportation Security Administration (TSA) had applied relatively uniform methods to screen airline passengers, focusing primarily on advances in screening technology to improve security and efficiency. TSA has recently shifted away from this approach, which assumes a uniform level of risk among all airline travelers, to one that focuses more intently on passengers thought to pose elevated security risks. Risk-based passenger screening includes a number of initiatives that fit within a broader framework addressing security risks, but specifically emphasizes the detection and management of potential threats posed by passengers.

Various risk-based approaches to airline passenger screening have been used since the early 1970s, including the application of rudimentary behavioral profiles, security questions, and analysis of ticket-purchase data to look for indicators of heightened risk. Additionally, "no-fly" lists were developed to prevent known or suspected terrorists from boarding aircraft, but prior to the terrorist attacks on September 11, 2001, these lists were not robust and proved ineffective.

Following the 9/11 attacks, TSA's initial risk-based efforts focused on integrating checks of passenger name records against the "no fly" list of individuals to be denied boarding and the "selectee" list of individuals of elevated risk requiring more thorough secondary screening. These efforts culminated in the deployment of Secure Flight, which screens each passenger's full name and date of birth against terrorist watchlists. Additionally, international passengers are screened by U.S. Customs and Border Protection (CBP), which uses the Advance Passenger Information System (APIS) and the Automated Targeting System-Passenger (ATS-P) to conduct risk assessments.

At airports, TSA employs behavioral detection and analysis under the Screening Passengers by Observational Techniques (SPOT) program in an effort to identify suspicious passengers. Another risk-based security program is Pre-Check, a trusted traveler program designed to expedite processing of low-risk passengers. In addition to the Pre-Check participants, TSA is routing certain other passengers through expedited lanes using behavior detection officers and canine teams to screen for suspicious behavior and explosives under an initiative called managed inclusion.

Implementation of risk-based passenger screening raises numerous issues of congressional interest. These include the efficacy of the SPOT program; how the various elements and programs complement each other and integrate with TSA's other layers of security; the risk-based approach's ability to adapt and evolve over time; the ability to measure its effectiveness; the potential impacts of false positives on the traveling public; and implications for safeguarding data and maintaining privacy.

Contents

Tables

Contacts

Airline Passenger Screening in the Post-9/11 Context

Airline passenger screening in the United States has been transformed since the 9/11 terrorist attacks. These transformations fall into two broad categories: new screening technologies, including advanced X-ray systems for screening carry-on items and whole-body scanners, and changes in policies, procedures, and practices such as requiring passengers to remove laptop computers and liquids from their carry-on luggage at the time of screening. These changes have been overseen by the Transportation Security Administration (TSA), the federal agency created in the aftermath of the 9/11 terrorist attacks under provisions in the Aviation Transportation and Security Act (ATSA; P.L. 107-71).

In ATSA, Congress mandated that TSA provide for comprehensive security screening of all airline passengers and property carried aboard passenger air carrier aircraft. ATSA, however, gave TSA authority to implement trusted traveler programs and utilize available technologies to expedite the security screening of passengers participating in such programs in order to allow screening personnel to focus on passengers who should be subject to more extensive screening. Subsequently, Congress (see P.L. 108-458) directed TSA to assume responsibility for checking all airline passengers against terrorist watchlists maintained by the federal government. Implementing these and other risk-based facets of passenger screening proved to be extremely challenging. Consequently, TSA has mostly relied on an assumption of uniform risk among airline passengers in its approach to airport checkpoint screening. This stands in contrast to the risk-based strategies TSA has employed to address other aspects of aviation security, such as air cargo security and security of charter and non-commercial operators.

Technologies such as whole-body imagers and advanced X-ray equipment have improved detection of a broad array of threat objects, including non-metallic weapons and explosives, but technology limitations, budgetary considerations, and other factors have placed constraints on a strictly technology-driven approach.

The uniform approach to screening has proven problematic. Under this approach, efforts to improve screening capabilities and streamline the screening process have primarily focused on technology. Technologies such as whole-body imagers and advanced X-ray equipment have improved detection of a broad array of threat objects, including non-metallic weapons and explosives, but technology limitations, budgetary considerations, and other factors have placed constraints on a strictly technology-driven approach to airport screening. TSA personnel have limited time and resources to screen passengers and property at airports without creating unacceptably long wait times. Space limitations at airports and congressional limitations on screener hiring have constrained TSA's capability to address these concerns simply by adding screening lanes and personnel.[1] Airline passengers continue to face sometimes cumbersome procedures, such as removing shoes and separating laptop computers for X-ray screening, that can make airport wait times unpredictable and even deter travelers from flying.

Inflexible security methods may have tainted public perceptions of TSA—a 2012 poll showed 54% of Americans thought TSA was doing a good or excellent job[2]—and led to sharp criticism

[1] See, e.g., P.L. 113-6, which prohibited FY2013 recruiting or hiring that would result in TSA exceeding a staffing level of 46,000 full-time equivalent screeners.

[2] Frank Newport and Steve Ander, *Americans' Views of TSA More Positive Than Negative*, Gallup, Princeton, NJ, August 8, 2012, http://www.gallup.com/poll/156491/Americans-Views-TSA-Positive-Negative.aspx.

from experts such as former TSA Administrator Kip Hawley, who has argued, "In attempting to eliminate all risk from flying, we have made air travel an unending nightmare ..., while at the same time creating a security system that is brittle where it needs to be supple."[3]

TSA has responded to such criticisms by attempting to shift from an approach that assumes a uniform level of risk among all airline travelers to one that focuses on passengers thought to pose elevated security risks. Risk-based screening has itself been controversial; while some initiatives have been encouraged or even directed by Congress, others have met with considerable skepticism among some Members of Congress or outside groups. The controversy derives, in part, from widely divergent views of what constitutes risk and how risk should be appropriately assessed and mitigated.

What Is Risk?

The dilemma over where to appropriately focus security efforts can be informed by the advice Frederick the Great offered to his generals: "Little minds try to defend everything at once, but sensible people look at the main point only; they parry the worst blows and stand a little hurt if thereby they avoid a greater one. If you try to hold everything, you hold nothing."[4] That view was echoed more recently by former Secretary of Homeland Security Michael Chertoff, who wrote in 2006, "In a free and open society, we simply cannot protect every person against every risk at every moment in every place. There is no perfect security."[5]

While security is necessarily imperfect, it nonetheless can be configured in an informed manner designed to minimize risk. The preliminary step in this process is to reach an understanding of the nature and characteristics of the security risk, followed by an identification of specific strategies to mitigate or manage that risk.

In the aviation security context, risk is often framed as a complex interaction of three underlying factors: threats, vulnerabilities, and consequences.

A general definition of risk focuses on the probability of incurring some type of loss. In the aviation security context, risk is most often framed as a complex interaction of three underlying factors: threats, vulnerabilities, and consequences.[6] Although risk is a probabilistic construct, the ability to assign specific probability values to individual threats and vulnerabilities in the aviation security context is limited. Consequently, risk-based practices settle for categorical techniques and scoring methods to quantify threats, vulnerabilities, and security risk in less precise terms.

A comprehensive risk-based aviation security strategy attempts to mitigate all three elements of risk. Risk-based passenger screening includes a number of initiatives that fit within this broader framework, but it focuses specifically on detecting and managing the threat element of risk.

[3] Kip Hawley, "Why Airport Security Is Broken – And How To Fix It," *Wall Street Journal,* April 15, 2012.

[4] Frederick the Great, as quoted in Peter G. Tsouras (Ed.), *The Greenhill Dictionary of Military Quotations,* Greenhill Books (London, 2000).

[5] Michael Chertoff, "There is No Perfect Security," *Wall Street Journal,* February 14, 2006.

[6] U.S. Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine*, April 2011.

Risk is mitigated by identifying individuals who may pose threats and utilizing detection technologies to screen for weapons, explosives, and other threat objects. Vulnerabilities are identified through various assessment techniques and addressed through multiple layers of security, such as reinforcing cockpit doors, deploying air marshals aboard planes, and changing security protocols based on known or perceived threats.

In contrast to threat and vulnerability, consequences are generally assessed in terms of their potential severity, often to derive a risk valuation and assess costs and benefits of specific security strategies. Consequences, however, are primarily mitigated by emergency management and response and post-incident recovery activities. These activities are primarily the responsibility of airports, airlines, and state and federal emergency management agencies, and are not a principal concern of TSA.

Defining the risk environment and specifying acceptable and unacceptable levels of risk are key challenges in establishing an effective risk-based strategy for aviation security. With respect to air cargo security, TSA has made extensive use of risk scoring to assess risks and plan security strategy. With respect to commercial passenger aviation, however, the practice of risk scoring of individuals has been considered so complex and controversial that it has not been a central part of TSA's strategy. Rather, risk assessment[7] of airline passengers is performed primarily through categorical processes, such as by assigning passengers to low-threat, unknown or elevated threat, and high threat categories after checking biographical data against terrorist and criminal databases. Risk-based techniques also examine some behavioral indicators, such as ticket purchasing characteristics and overt behaviors exhibited at the airport. These indicators are used to derive behavioral-based risk scores, but the validity of these methods has been questioned.[8]

There may not be agreement on what specific risks a risk-based security strategy should seek to mitigate.

Complicating matters further, there may not be agreement on what specific risks a risk-based security strategy should seek to mitigate. One example of this occurred following TSA's March 2013 proposal to allow passengers to carry small knives and certain sports equipment onboard aircraft, reversing a long-standing ban. The agency asserted that the threat posed by these items had diminished and that other security layers, such as deployment of armed air marshals aboard some flights, arming of some pilots through the Federal Flight Deck Officers (FFDO) program, and reinforcement of cockpit doors sufficiently mitigated the risk of a hijacking or terrorist attack posed by small knives, golf clubs, and baseball bats. Critics, including organizations representing flight attendants, pilots, and airlines, argued that TSA had failed to adequately consider risks unrelated to hijacking and terrorism, such as those posed by unruly passengers wielding knives and golf clubs aboard planes. After legislation was introduced to prevent TSA from lifting its ban on small knives, TSA announced that it would not proceed with its proposal.[9]

[7] Although this is generally termed "passenger risk assessment" rather than "passenger threat assessment," the technique focuses exclusively on the potential threat posed by an individual passenger. The terms are interchangeable in this context given an assumption that other aspects of risk besides threat (i.e., vulnerability and severity of consequences) are held constant.

[8] See, e.g., U.S. Government Accountability Office, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013.

[9] Bart Jansen, "TSA Drops Efforts to Allow Small Knives on Planes," *USA Today,* June 5, 2013.

Elements of Risk-Based Security

Risk-based passenger screening stands in contrast to TSA's historical approach of prohibiting certain items aboard aircraft and instructing screeners to focus on enforcing those prohibitions.

At the operational level, risk-based passenger screening stands in contrast to TSA's historical approach of prohibiting certain items aboard aircraft and instructing screeners to focus on enforcing those prohibitions. This comports with the concerns raised by former TSA administrator Hawley, who wrote of the dilemma faced by TSA screeners, "the fear of missing even the smallest thing, versus the likelihood that you'll miss the big picture when you're focused on the small stuff."[10]

Hawley's objections are shared by Raphael Ron, an Israeli expert on aviation security and counterterrorism. Ron asserts that reliance on prohibited items lists and detection technology reduces the security system's ability to respond to shifting threat landscapes; he notes that the box cutters used by hijackers in the 9/11 attacks were not prohibited items at the time. As he writes, "Terrorists love our detection technology because they can trust that it will not do what it is not designed to do and never did before. In a sense, our technology gives the terrorist a positive feedback on what to expect." Ron claims that there has never been a case in which a planned terrorist attack was prevented by the detection of threat items alone.[11]

Comments such as Hawley's and Ron's point to an approach that does not dispense with detection technologies, but integrates detection capabilities with other measures for assessing threats and minimizing vulnerabilities. Such an approach might depart from TSA's historical practice of using relatively rigid and inflexible measures to screen passengers in a uniform manner. They might require the agency to be more proactive, as opposed to largely reactive, with respect to specific threats and incidents, and to emphasize flexibility and unpredictability.

Advocates of risk-based security frequently point to Israel, which employs demographic profiling, intelligence and law enforcement databases, and extensive security interviews to identify passengers deemed to pose high risks. These individuals are then subject to heightened screening measures and in-depth inquiries to assess any potential threat before they are allowed to board a plane. Despite continued threats, Israel has avoided any major terrorist attacks against its airlines and airports for over 40 years. The exact role that its methods have played in deterring or preventing such attacks is undetermined. Regardless, adopting an Israeli-style approach in the United States is considered to be problematic, both legally and pragmatically. Research by TSA's Kenneth Fletcher concluded that a risk-based approach to passenger screening tailored to meet the specific operational and legal framework of aviation security in the United States would be more effective, as well as more politically feasible, socially acceptable, and legally defensible, than the extensive interviewing and targeted screening carried out under the Israeli airport security model.[12]

[10] Kip Hawley, "Why Airport Security Is Broken – And How To Fix It," *Wall Street Journal,* April 15, 2012.

[11] Raphael Ron, "Airport Security: A National Security Challenge," Policy Brief, International Border Security Forum, Washington, DC: The German Marshall Fund of the United States, May 2013.

[12] Kenneth C. Fletcher, "*Aviation Security: A Case for Risk-Based Passenger Screening,"* Thesis, Naval Postgraduate School, Monterey, CA, December 2011.

Table 1 identifies the principal attributes of a comprehensive risk-based aviation security framework, as described by scholars of the subject.

Table 1. Attributes of a Comprehensive Risk-Based Approach to Security

Attribute	Description
Intelligence Driven	Intelligence information and analysis including both threat and vulnerability assessments informs decisions regarding security policies, procedures, practices, and postures.
Unpredictable	Elements of the security system should not be routine, predictable, or overly rigid, and should maintain some degree of random assignment to various screening techniques. Procedures attempt to minimize the opportunity for adversaries to test the system in an effort to uncover latent vulnerabilities.
Adaptable	The security system is not overly rigid and can adapt, sometimes on very short notice, to a changing threat picture. Moreover, implementation must adapt to cultural norms, societal constraints, and legal processes, which may also shift over time.
Evolving	The security system is not overly rigid, but rather is capable of evolving to incorporate new technologies, new approaches, and changing threat landscapes.
Layered	The security system incorporates multiple elements, relatively independent and isolated from one another, and employs redundancies implemented in a coordinated manner so that a failure of one component does not expose the entire system to an unacceptable level of risk.

Source: CRS analysis, based on Raphael Ron, "Airport Security: A National Security Challenge," Policy Brief, International Border Security Forum, Washington, DC: The German Marshall Fund of the United States, May 2013; Kenneth C. Fletcher, "Aviation Security: A Case for Risk-Based Passenger Screening," thesis, Naval Postgraduate School, Monterey, CA, December 2011; and Bartholomew Elias, *Airport and Aviation Security: U.S. Policy and Strategy in the Age of Global Terrorism* (Boca Raton, FL: CRC Press, 2010), pp. 133-158.

Risk-based screening should be understood as part of a comprehensive, multi-layered approach to aviation security rather than as an alternative approach. Risk-based programs closely interact with physical screening checkpoint measures to allow TSA to focus physical screening resources on unknown and elevated risk passengers. They also inform the protocols TSA utilizes to modify security postures based on known or perceived threats. It is possible that risk-based programs affect decisions related to the posting of behavioral detection officers and the deployment of air marshals by identifying which passengers should be more closely observed and which flights may be considered high-risk, although details about the interaction of these security components have not been disclosed publicly.

Risk-Based Approaches Applied to Airline Passengers

Risk-based approaches to airline passenger screening have been used since the early 1970s. At that time, before 100% screening of all airline passengers went into effect in 1973, the Federal Aviation Administration (FAA) used rudimentary passenger profiles to determine whether to screen particular passengers and search their carry-on items.[13] In the late 1970s, as walk-through metal detectors and X-ray scanners for carry-ons were deployed at commercial passenger airports and became mandatory, these risk-based profiling techniques were largely abandoned, although FAA continued to utilize profiling tools to examine information in airlines' passenger name records that could signal an increased threat.

In the late 1980s, concern over aircraft bombings led FAA to require that airlines ask all passengers two basic security questions:

- Has anyone unknown to you asked you to carry any items on this flight?
- Have any of the items you are traveling with been out of your immediate control since the time you packed them?

The questions served for years as rudimentary security screening measures, primarily to target elevated-risk checked baggage, but were often criticized because their intent seemed so obvious and they were typically posed by airline ticket agents with little or no security training. Nonetheless, they served to heighten passenger awareness of potential security threats and reflected the real threat posed by bombers who may try to dupe an unwitting individual into carrying a device aboard an aircraft (see **Text Box**). Although several other countries and some foreign airlines continue to use these or similar questions, usually as part of more in-depth interviews or questioning conducted by security screeners, TSA eliminated use of the questions in 2006.[14]

[13] Bartholomew Elias, *Airport and Aviation Security: U.S. Policy and Strategy in the Age of Global Terrorism* (Boca Raton, FL: CRC Press, 2010).

[14] ABC News, "Airline Security Questions Scrapped," January 7, 2006, available at http://abcnews.go.com/US/story?id=91316&page=1.

Unwitting Bomb Carriers

On November 1, 1955, the crash of United Airlines Flight 629 killed all 44 on board shortly after departing Denver, CO. The cause of the crash was determined to be a dynamite bomb. John Gilbert Graham confessed to secretly placing the bomb in his mother's suitcase. He was convicted of killing his mother and was executed in 1957.

It has been speculated, but never proven, that the crash of National Airlines Flight 967 on November 16, 1959, was caused by a concealed explosive device brought aboard unknowingly by an ex-convict who was carrying a package given him by a friend from prison. The suspect is thought to have talked his friend into traveling on a ticket purchased in the suspect's name in a scheme to collect a life insurance payment. All 42 on board were killed when the aircraft crashed in the Gulf of Mexico on a flight from Tampa, FL, to New Orleans, LA.

On April 17, 1986, Israeli security officers conducting preflight interrogations of passengers at London Heathrow Airport found an improvised explosive device in a bag carried by a pregnant Irish woman. She claimed that the bag had been packed and given to her by her fiancé, a Jordanian national, who told her he would be traveling separately and would meet her later in Israel. The incident is frequently cited as an example of the effectiveness of Israel's airline security techniques and motivation for questioning all passengers about the contents of their baggage.

Following the December 21, 1988, bombing of Pan Am Flight 103 over Lockerbie, Scotland, FAA and the airlines developed the Computer-Assisted Passenger Pre-Screening (CAPPS) system, which was implemented in the late 1990s. CAPPS resides on airline reservation systems and relies on patterns in flight reservation data to identify passengers considered to pose potential security threats. While the specific algorithms used by CAPPS, which is now overseen by TSA, are security sensitive, it has been reported that indicators may include purchasing a one-way ticket or paying with cash.[15] Separately, FAA, in coordination with the Federal Bureau of Investigation (FBI), developed a list of known terrorists who were to be denied boarding: the "no-fly" list. However, on the day of the 9/11 attacks only 12 names were on the list, none of them the 9/11 hijackers, even though other government terrorist watchlists contained tens of thousands of names.[16]

After the 9/11 attacks, ATSA directed TSA to establish requirements for trusted traveler programs and to use available technologies to expedite screening for participating passengers, thereby allowing screening personnel to focus on those passengers who should be subject to more extensive screening. The act, along with the subsequent Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), directed TSA to ensure that CAPPS or any successor system be used to evaluate all passengers prior to boarding, and to assure adequate screening of passengers selected by such systems as well as their carry-on and checked baggage. This emphasis on risk-based screening reflected recommendations made by the Department of Transportation Airport Security Rapid Response Team, formed in response to the 9/11 attacks. Specifically, the team found an urgent need to establish a nationwide program for voluntarily submitting information for vetting passengers in order to expedite processing of the vast majority of travelers, thus allowing aviation security resources to be focused more effectively. The team also recommended that passenger prescreening performed using CAPPS be applied to assess passenger risk on all flights.[17]

[15] Ryan Singel, "Life After Death for CAPPS II?" *Wired,* July 16, 2004.

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

[17] U. S. Department of Transportation, *Meeting the Airport Security Challenge: Report of the Secretary's Rapid Response Team on Airport Security,* October 1, 2001.

In response to these mandates, TSA initiated work on a follow-on system to CAPPS. Dubbed CAPPS II, the system endeavored to encompass identity authentication, watch list checks, and expanded risk-based assessments of passengers. As initially envisioned, CAPPS II was to integrate checks of passenger name records against the "no fly" list of individuals to be denied boarding and the "selectee" list of individuals of elevated risk requiring more thorough secondary screening. It was to include the capability to categorize or score passengers based on threat assessments, potentially using additional government and commercial databases. Controversy over privacy, data protection, and redress processes led TSA to scrap CAPPS II development in 2004, and move forward with a more focused effort to screen all passengers against terrorist watchlists.

Secure Flight

Despite missteps in developing CAPPS II, the 9/11 Commission formally recommended in 2004 that the "no fly" and "automatic selectee" lists be improved, and that air passengers be screened not only against these lists, but against the "larger set of watchlists maintained by the federal government."[18] The commission urged that screening be performed by TSA, not by air carriers, and that carriers be required to supply the information needed to test the new prescreening system.

Reflecting the recommendations of the 9/11 Commission, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required TSA to assume the passenger watchlist screening function from air carriers, after it established a way to utilize the greater set of watchlists integrated in the Terrorist Screening Database (TSDB) administered by the FBI.

Reflecting the recommendations of the 9/11 Commission, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required TSA to assume the passenger watchlist screening function from air carriers, after it established a way to utilize the greater set of watchlists integrated in the Terrorist Screening Database (TSDB) administered by the FBI. Appropriations language, however, expressly forbade TSA from employing algorithms to assign risk scores to passengers or from using commercial data other than airline passenger name records in assessing passenger risk.[19]

In October 2008, TSA published a final rule detailing the operational implementation of this program, which it called "Secure Flight."[20] The program was implemented for domestic flights in 2009 and for international flights in 2010. Secure Flight has been fully operational since 2011, screening passenger biographic information against terrorist watchlists, principally the TSDB. The "no fly" and "selectee" (or "automatic selectee") lists are subsets of this database. While the specifics are classified, TSA said in 2008 that the full TSDB contained fewer than 400,000 names, of which about 50,000 identities were included in either the "no fly" or "selectee"

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

[19] See, e.g., P.L. 109-90, §518.

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

subsets.[21] More recently, the news media reported in May 2013 that the larger Terrorist Identities Datamart Environment, or TIDE—a repository maintained by the National Counterterrorism Center that serves as a principal source of foreign identities included in the TSDB—has grown to include about 875,000 names.[22] TIDE serves as a principal data source for foreign terrorist identities included in the TSDB. The expansion of TIDE was attributed in large part to increased reliance on the system in the aftermath of the failed bombing attempt on Northwest Flight 253 on December 25, 2009, and subsequent reviews of intelligence community practices. The TSDB has also expanded, reportedly containing more than 500,000 identities as of September 2012, as improving watchlist practices, with a particular emphasis on processing nominations and removals to assure timeliness, accuracy, and completeness, has been a significant focus of intelligence community efforts since the attempted bombing.[23]

Functionally, Secure Flight compares data from airline passenger name records against the "no fly" and "selectee" lists, and in certain cases, against the full TSDB, to determine whether passengers and other individuals seeking access through airport checkpoints (such as family members assisting disabled travelers or children traveling as unaccompanied minors) should be denied access or subject to additional screening measures. Additionally, Secure Flight compares passenger names to a list of individuals provided by the Centers for Disease Control and Prevention of persons who should be denied boarding due to public health concerns.[24]

If TSA does not identify a potential watchlist match using Secure Flight, records are to be destroyed within seven days of completion of the travel itinerary. Potential matches, however, are retained for 7 years and confirmed watchlist matches may be retained for up to 99 years. Known traveler lists and lists of individuals disqualified from expedited screening due to past security incidents are retained until superseded by updated lists.[25]

Pre-Screening International Passengers

Secure Flight development benefited from operational experience with the Advance Passenger Information System (APIS) administered by U.S. Customs and Border Protection (CBP), which predated Secure Flight and continues to collect passenger manifest data from airlines for all international flights inbound to the United States. Air carriers transmit APIS data on passengers and crew to CBP prior to aircraft departure. CBP cross-checks the data against law enforcement, customs, and immigration screening databases and terrorist watchlists.

[21] Transportation Security Administration, "Myth Buster: TSA's Watch List is More Than One Million People Strong." *The TSA Blog,* July 14, 2008, available at http://blog.tsa.gov/2008/07/myth-buster-tsas-watch-list-is-more.html.

[22] Mark Hosenball, "Number of Names on U.S. Counter-Terrorism Database Jumps," Reuters, May 2, 2013.

[23] U.S. Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Management of Terrorist Watchlist Nominations,* Audit Report 14-16, March 2014.

[24] The public health Do Not Board (DNB) list includes the names of individuals with communicable diseases who pose a serious threat to the public. The Centers for Disease Control and Prevention reviews all requests to place a name on the list to verify that the individual meets the appropriate medical criteria for inclusion. In the first year following creation of the list in 2007, 42 names were submitted and 33 names were placed on the list, all referencing individuals thought to have infectious pulmonary tuberculosis.

[25] Transportation Security Administration, "Privacy Act of 1974: System of Records; Secure Flight Records," 77 *Federal Register* 69491-69496, November 19, 2012.

CBP also relies on its Automated Targeting System-Passenger (ATS-P) to perform risk assessments on inbound and outbound international travelers. For inbound flights, ATS-P serves as a tool to assist CBP in making assessments in advance of arrival as to whether an individual should be admitted to the United States. Derived from a system developed in the 1990s to identify suspect cargo, the passenger module of ATS does not use a risk scoring methodology to determine an individual's risk. Rather, it compares elements of passenger name record data for all travelers against terrorist and law enforcement databases to identify potential matches to terrorist identities and wanted criminals, and to look for other red flags such as suspected use of a lost or stolen passport. In contrast, the cargo screening module of ATS relies on risk scoring methods.

In general, data in the ATS may be retained for up to 15 years.[26] In accordance with an agreement between the United States and the European Union, however, passenger name record data are depersonalized within six months, but may otherwise be retained in an active database for up to five years. Thereafter, the data will be transferred to a dormant database, where they may be retained for up to 10 years.[27]

Additionally, travelers with passports from countries in the Visa Waiver Program[28] must electronically submit biographical information through the Electronic System for Travel Authorization prior to boarding a U.S.-bound flight.[29] That information is checked against law enforcement databases, databases of lost and stolen passports, visa revocations, and the TSDB. For each passenger, CBP transmits the resulting status code to Secure Flight specifying whether the database checks indicate a potential threat.

Screening Passengers by Observational Techniques (SPOT)

Secure Flight seeks to employ risk-based analysis drawing exclusively on data compiled by government agencies and the airlines. A separate TSA program, Screening Passengers by Observational Techniques (SPOT), attempts to identify passengers who could present threats by observing behavior at airports. TSA initiated early tests of SPOT in 2003. By FY2012, the program deployed almost 3,000 BDOs at 176 airports, at an annual cost of about $200 million. Program costs and continued questions over its scientific validity and operational utility have been central concerns in the continued controversy over the program since its inception. TSA asserts that its behavior detection and analysis program is "based on scientifically validated behaviors to identify individuals who potentially pose a threat to the nation's transportation network."[30]

SPOT is rooted in law enforcement techniques that rely on criminal profiling methods and behavioral assessment strategies, including behavioral observation. TSA asserts that behavior

[26] Department of Homeland Security, "Privacy Act of 1974; U.S. Customs and Border Protection, DHS/CBP-006—Automated Targeting System, System of Records," 77 *Federal Register* 30297-30304, May 22, 2012.

[27] See CRS Report RS22030, *U.S.-EU Cooperation Against Terrorism*, by Kristin Archick.

[28] See http://travel.state.gov/content/visas/english/visit/visa-waiver-program.html

[29] For more information see CRS Report RL32221, *Visa Waiver Program*, by Alison Siskin.

[30] Transportation Security Administration, Statement of Administrator John S. Pistole, Before the United States House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, November 13, 2013.

detection techniques that form the basis for SPOT have been practiced for many years in the context of law enforcement, customs and border protection, defense, and security. However, there are several nuanced differences between SPOT and law enforcement behavior analysis tools and techniques that set the SPOT program apart.

Law enforcement agencies generally apply behavioral analysis in the investigation of specific crimes, not with large groups of individuals, and tend to employ extensive interviewing methods to look for patterns of inconsistencies in statements and to gather evidence for potential criminal proceedings. Moreover, whereas behavioral detection as practiced in the TSA SPOT program focuses heavily on interpretation of non-verbal cues, such as facial expressions or avoidance of eye contact, such cues generally do not play a central role in establishing suspicion in a law-enforcement setting. In this regard, TSA's SPOT program stands out as unique in its extensive use of non-invasive observation techniques and its development of a formal scoring system to rate suspicion on the basis of behavioral indicators, including non-verbal indicators evaluated by a behavior detection officer. Whereas law enforcement agencies will use such techniques in combination with other interrogation practices, often over the course of lengthy interviews and repeated encounters with persons of interest, TSA has stated that it takes a BDO less than 30 seconds to meaningfully observe an average passenger.[31]

TSA's SPOT program stands out as unique in its extensive use of non-invasive observation techniques and its development of a formal scoring system to rate suspicion on the basis of behavioral indicators, including non-verbal indicators evaluated by a behavior detection officer.

Since its inception, reviews of the SPOT program have raised questions regarding whether it is an effective tool for identifying individuals who pose a specific threat to aviation. Despite TSA's assertions regarding effectiveness, the Government Accountability Office (GAO) reported in 2010 that on at least 23 different occasions, at least 16 known terrorists transited through checkpoints at eight different airports where BDOs were stationed. GAO could not determine if the SPOT program had resulted in the arrest of any terrorists or individuals planning to engage in terrorist activity. It concluded that the SPOT program had been fielded before being fully validated and without adequate cost-benefit analysis.[32]

TSA responded by carrying out validation studies in cooperation with the Department of Homeland Security (DHS) Science and Technology Directorate and the American Institutes for Research. According to TSA, the tests demonstrated that its behavior detection techniques were nine times more likely to detect high-risk travelers than random selection. It has not released the study publicly to allow for independent analysis or critique.[33] The agency also said it had taken specific steps to address GAO recommendations for improving behavior assessment methods, performance metrics, data collection, and program management. Further, TSA noted that it has partnered with several international counterparts to exchange operational and programmatic information and share best practices to further refine the SPOT program.

[31] U.S. Government Accountability Office, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013.

[32] U.S. Government Accountability Office, *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, GAO-10-763, May 2010.

[33] Transportation Security Administration, Statement of Administrator John S. Pistole, Before the United States House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, November 13, 2013.

Despite the seemingly impressive results of the validation study reported by TSA, both the GAO and the DHS Office of Inspector General have continued to raise doubts about behavior detection and analysis as employed in the SPOT program. In 2013, GAO concluded that available evidence still did not support the validity and utility of behavior detection techniques employed by TSA.[34] A fundamental concern was that the metrics TSA used to evaluate the program—principally, the number of referrals to law enforcement that have resulted in confiscations of prohibited items or arrests and detentions for warrants, parole violations, drug possession, other criminal activity, and illegal immigration status—do not directly relate to TSA's mission to deter, detect, and prevent terrorism and other criminal acts targeting aviation assets. Given the low occurrence of terrorist acts, developing suitable metrics to evaluate the impact of the SPOT program on these mission objectives has proven elusive. GAO reported wide individual differences among BDOs in terms of referrals to law enforcement, raising questions about the training on and operational use of behavioral indicators.

Similarly, the DHS Office of Inspector General found that metrics used to support TSA's assertion of SPOT's effectiveness, such as detection of prohibited items, undeclared currency, and illegal aliens, are not directly related to aviation security objectives. Its audits revealed significant lapses in records-keeping, suggesting that incomplete and inaccurate data about the program had been presented to TSA's senior leadership. The Inspector General also found that TSA did not consistently offer formal refresher training for behavior detection officers, despite a TSA task force's conclusion that "observation skills ... need to be constantly honed and refocused on some regular basis."[35] Moreover, a lack of performance evaluation and recurrent training for BDO instructors raised additional questions about the quality and consistency of BDO training.

While TSA has championed the SPOT program as a cornerstone of its risk-based approach to passenger screening, questions remain over the program's efficacy.

While TSA has championed the SPOT program as a cornerstone of its risk-based approach to passenger screening, questions remain over the program's efficacy. While some Members of Congress have sought to shutter the program, Congress has not moved to do so. For example, H.Amdt. 127, an amendment to the FY2014 DHS appropriations measure which sought to eliminate funding for the program, failed to pass a floor vote.[36] Congress also has not taken specific action to revamp the program, despite the concerns raised by GAO and the DHS Office of Inspector General.

[34] U.S. Government Accountability Office, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013.

[35] Department of Homeland Security, Office of Inspector General, *Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted)*, OIG-13-91, Washington, DC, May 29, 2013; Department of Homeland Security, Statement of Charles K. Edwards, Deputy Inspector General, Before the United States House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, November 13, 2013.

[36] See Rep. John Carter, "Department of Homeland Security Appropriations Act, 2014," House of Representatives, *Congressional Record*, Vol. 159, Issue 78 (June 5, 2013), p. H3194.

The Pre-Check Program

While behavioral detection approaches have been sharply criticized, TSA's efforts to implement Pre-Check, a trusted traveler program designed to expedite processing of low-risk passengers, have garnered more favorable responses. Pre-Check began in October 2011, and became fully operational in 2012. Since then, TSA has been incrementally expanding its scope and availability. The program is available at no cost to U.S. citizens designated as select frequent flyers of certain airlines, and to U.S. and Canadian citizens who are paid members of CBP's trusted traveler programs (including Global Entry, SENTRI, and NEXUS). Eligible travelers not in any of these categories may, for a fee, apply directly at a TSA enrollment center to join Pre-Check.

The Pre-Check program bears some resemblance to the former Registered Traveler (RT) program, which was scrapped in 2009. RT was implemented under a public-private partnership model with multiple vendors providing biographical and biometric data collection and storage. While different vendors held contracts to issue biometric IDs and operate identity verification kiosks at different airports, the systems were designed to be interoperable, theoretically giving registered travelers access to expedited screening lanes at multiple airports. When RT was launched at 19 airports in 2007, TSA conducted extensive background checks of applicants based on biographical data collected by vendors. However, as it expanded the program to additional airports in 2008, TSA eliminated the background check process and the associated portion of the program fee, indicating that these checks "were not core elements in determining threats,"[37] as terrorist watchlist checks were being performed on all passengers under Secure Flight. The program was dismantled shortly thereafter.

Under Pre-Check, TSA has resurrected extensive biographic-based background checks, apparently reversing its earlier stance under RT that these additional checks were of limited value in identifying threats to aviation security. In contrast to RT, Pre-Check does not issue a biometric credential. Rather, an approved individual is issued a known traveler number to use when booking flight reservations. This number is used to indicate the individual's status as a Pre-Check member on the boarding pass, thereby allowing the passenger to use expedited screening lanes. Nonetheless, to deter exploitation of expedited screening lanes, Pre-Check participants may be selected randomly to undergo more thorough physical screening.

The exclusive reliance on boarding passes for Pre-Check authentication may be of concern, given continued limitations in TSA's capability to authenticate boarding passes and traveler identification documents.

The exclusive reliance on boarding passes for Pre-Check authentication may be of concern, given TSA's limited ability to authenticate boarding passes and traveler identification documents. TSA's deployment of document and boarding pass inspection and authentication technologies, called Credential Authentication Technology/Boarding Pass Scanning Systems, has been delayed and faces several ongoing technical and managerial challenges.[38] Without the ability to authenticate boarding pass

[37] Transportation Security Administration, "TSA Lifts Cap and Eliminates Fee on Registered Traveler," Press Release, July 24, 2008; see also Transportation Security Administration, "Registered Traveler Interoperability Pilot Program," 73 *Federal Register* 44275-44278.

[38] U.S. Government Accountability Office, *Aviation Security: Status of TSA's Acquisition of Technology for Screening Passenger Identification and Boarding Passes*, GAO-12-826T, June 19, 2012.

information, TSA may not be able to assure that access to Pre-Check screening lanes is limited to properly cleared individuals at all airports.

In September 2013, TSA issued a system of records notice (SORN) regarding the process for members of the public to voluntarily apply for the Pre-Check program. The SORN defines the legal context under which TSA collects and retains information on Pre-Check applicants. Applicants are required to submit biographic and biometric data (i.e., fingerprints and identity verification documentation containing a photograph, such as a passport or driver's license) to TSA. TSA, in turn, is to use the submitted information to conduct security threat assessments of individuals, using law enforcement, immigration, and intelligence databases, including a fingerprint based criminal history records check through the FBI.

TSA accepts Pre-Check applications from U.S. citizens, U.S. nationals, and legal permanent residents. Individuals are to be determined ineligible if, within specified time periods (generally seven years since court determination or five years since release from prison), they have been convicted of, found not guilty by reason of insanity, or are under want, warrant, or indictment for certain specific crimes. Further, TSA may reject an applicant with extensive foreign or domestic criminal convictions, even if the crimes are not specifically disqualifying, and may reject an applicant based on information in government terrorist watchlists, Interpol data, and other international law enforcement and counterterrorism data.

Pre-Check applicants must pay a non-refundable processing fee of $85. Once vetted and approved, a traveler is to receive a notification letter from TSA with an assigned Pre-Check Known Traveler Number, which will be valid for five years. Applicants who are determined not to be qualified for Pre-Check must notify TSA within 30 days to indicate their intent to appeal and to correct information believed to be inaccurate. To obtain corrections, the applicant must provide certified copies of records supporting the claim that the initial determination was inappropriate. Since the $85 processing fee is non-refundable, individuals who have reason to believe they may be disqualified based on their criminal record or may not meet eligibility requirements because of other factors, including citizenship or residency status, may choose not to apply.

In December 2013, TSA opened the first Pre-Check enrollment center for the general public at the Indianapolis, IN, airport. TSA anticipates that there will eventually be as many as 300 enrollment centers nationwide as well as an online application process. Individuals seeking to participate may initiate the application process by pre-enrolling online, but must visit a physical enrollment site to provide identification and fingerprints.

Early indications have suggested that frequent travelers are generally pleased with Pre-Check. A 2012 survey of frequent flyers found that almost 54% of those using Pre-Check were very satisfied or extremely satisfied, compared to less than 7% of frequent travelers expressing similar opinions of their most recent TSA screening in general.[39]

However, rapid expansion of the program could limit some of its benefits.[40] TSA has increased availability of Pre-Check's expedited screening lanes from 40 airports in FY2013 to over 100

[39] Dan Collins, "Poll: 90% of Frequent Flyers Give TSA Fair or Poor Rating," *Frequent Business Traveler,* September 10, 2012.

[40] Bart Jansen, "Privacy Concerns Swirl Around TSA Pre-Check Program," *USA Today*, February 24, 2014.

airports by January 2014, with a goal of providing expedited screening to half of all airline passengers by the close of FY2015. As the Pre-Check program grows in popularity, wait times in Pre-Check lanes may increase, while non-participating travelers may potentially stand to save time also as more and more fellow travelers join Pre-Check. Non-participating travelers may also benefit from possible selection to use a Pre-Check lane either through occasional selection based on Secure Flight assessments or under an initiative referred to as managed inclusion.

Managed Inclusion

Managed inclusion refers to a TSA initiative exploring real-time threat assessments of passengers to identify individuals considered low risk and thus eligible for random selection for processing using one of the Pre-Check expedited screening lanes. New passenger screening canine teams, specially trained to work in crowded areas and sniff passengers to detect the scent of explosives, along with behavioral detection officers who screen individuals for behavioral indicators of potential threat, perform initial screening of passengers in the screening checkpoint queue. If neither the canine team nor the officer signals that a passenger is an elevated risk, then he or she may be randomly selected for managed inclusion in a Pre-Check screening lane. Upon stepping on a mat in front of the travel document checker's kiosk the passenger triggers a lighted directional arrow that will indicate whether to proceed to regular screening lanes or a Pre-Check expedited screening lane, based on a random selection.

Military Members, Department of Defense Civilians, and Known Crewmembers

In addition to Pre-Check members and those selected by Secure Flight selection or managed inclusion, military servicemembers, including active duty members, reservists, and National Guard members, are allowed to use Pre-Check screening lanes. Cleared military personnel can use this service for both official and personal travel. Family members under 12 years old may pass through the Pre-Check lanes when traveling with cleared military personnel. However, family members over age 12 must either proceed through standard screening lanes or independently obtain eligibility for the Pre-Check program through the various means established by TSA. It has been reported that civilian employees of the Department of Defense and the Coast Guard will also be allowed to participate in expedited screening beginning in mid-April 2014 without enrolling in Pre-Check or a CBP trusted traveler program.[41]

Pre-Check lanes are also being used to expedite screening of uniformed airline crewmembers, including pilots and flight attendants, participating in TSA's Known Crew Member identification initiative. Airline-issued identification credentials are to be checked against a database of participating airlines' flight and cabin crew personnel with valid security background checks to determine eligibility for expedited screening. Airline crews undergo TSA managed fingerprint-based criminal history record checks and security threat assessments as a condition of employment.[42] The Known Crew Member database can serve as a means of verifying airline crew credentials and eligibility for expedited screening.

[41] Josh Hicks, "TSA's expedited screening lanes soon open to DOD and Coast Guard civilians," *Washington Post*, March 27, 2014.

[42] See 49 CFR §1544.229 and §1544.230.

Each of these sub-populations undergoes background screening that, at a minimum, TSA considers equivalent to those performed on Pre-Check applicants. In many cases, particularly for military personnel and civilian employees holding defense secret clearances, the background investigation may be even more extensive, even though the security clearance process for these individuals has recently been criticized.[43]

TSA considers individuals in these specific sub-populations to be lower risk than individuals from the general population who have not undergone a background investigation, and of comparable risk to trusted travelers vetted directly by TSA or CBP. Moreover, the credentialing process for military servicemembers, defense personnel, and airline crews may be seen as providing a comparatively secure means of assuring an individual's identity and eligibility for expedited screening under these provisions. Nonetheless, TSA continues to use random selection to direct certain members of these sub-populations to standard non-expedited screening, as it does with Pre-Check members. This adds an unpredictable element to screening, in keeping with the principles of a comprehensive risk-based approach to security.

Collection and Retention of Passenger Data

Each risk-based screening program collects and retains various forms of biographic, biometric, and/or other identifying data regarding individuals. Additionally, TSA collects and retains data from intelligence sources and its own investigations regarding potential threats and identities of individuals believed to pose some level of threat to the aviation system. Each risk-based program has separate data collection and retention rules (see **Table 2**).

TSA has stated that its policy is to delete data that are no longer needed. Under the terms of its various SORNs, records that correspond to traveling individuals whose identities are matches or potential matches to terrorist or criminal databases are retained for extensive periods, whereas other records are destroyed shortly after completion of the corresponding travel itinerary. Data submitted voluntarily by individuals who are not considered possible matches, such as data provided in Pre-Check applications, are typically retained throughout an individual's participation in the program, unless superseded by updated or corrected data. While TSA may use information from commercial databases and consumer reporting agencies in validating identities and conducting risk assessments, it does not reciprocate by disclosing information to consumer reporting agencies.

[43] See, e.g., Christian Davenport, "Pentagon considers retaking control of security clearance checks," *Washington Post,* March 20, 2014.

Table 2. TSA and CBP Systems of Records Pertaining to Risk-Based Passenger Screening Programs

System of Records	Relevant Program(s)	Document Identification/ Federal Register Notice
Secure Flight Records	Secure Flight	DHS/TSA-019; 77 FR 69491 et seq.
TSA Pre-Check Application Program	Pre-Check	DHS/TSA-021; 78 FR 55274 et seq.
Transportation Security Enforcement Records System	SPOT, Federal Air Marshal Service (FAMS), Screeners	DHS/TSA-001; 75 FR 28042 et seq.
CBP Advanced Passenger Information System	CBP APIS	DHS/CBP-005; 73 FR 68435 et seq.
CBP Automated Targeting System	CBP ATS	DHS/CBP-006; 77 FR 30297 et seq.

Source: Department of Homeland Security, System of Records Notices (SORNs), available at http://www.dhs.gov/system-records-notices-sorns.

In general, personal data collected under these various risk-based programs may be shared among DHS agencies when necessary to support counterterrorism and homeland security mission functions. Data may also be shared with intelligence, law enforcement, and judicial agencies at the federal, state, local, or tribal levels for investigating potential criminal, civil, or regulatory violations, and with audit or oversight agencies, federal records management agencies, and federal contractors performing work that requires access to the specific data. In all these instances, data are to be protected against inappropriate handling or disclosure in accordance with the Privacy Act of 1974 (P.L. 93-579), in a manner detailed in each SORN.

Redress

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required 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 avoid recurrence. Also, provisions in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) required DHS to establish an Office of Appeals and Redress to establish a timely and fair process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat. DHS must maintain records of passengers and individuals who have been misidentified and have corrected erroneous information.

To meet these statutory requirements, DHS established the DHS Traveler Redress Inquiry Program (DHS TRIP) as a mechanism for addressing situations in which individuals claim to have been inappropriately singled out. The DHS TRIP program allows passengers seeking redress, or their representatives, to file complaints online or by mail.[44] After receiving the completed online questionnaire or the complaint form, DHS is to request supporting information within 30 days. Filers are given a control number that allows them to track the status of their inquiry using the Internet. If the investigation finds that the traveler was delayed due to a misidentification or name-matching issue, DHS is to describe the steps required to resolve the

[44] Complete instructions for filing complaints under the DHS TRIP program can be found at http://www.dhs.gov/one-stop-travelers-redress-process.

issue. For example, the traveler may be required to retain a copy of the DHS response letter and present it during the check-in process when traveling on airline flights. If a passenger disagrees with the resolution decision made by DHS, he or she may take further steps to appeal the decision. However, TSA decisions based on records maintained on individuals in connection with the Secure Flight program are largely exempt from judicial review.[45]

Analyzing Non-Governmental Data Using Third-Party Prescreening

In January 2013, TSA released a market research announcement seeking information to expand expedited screening beyond the Pre-Check program by relying on third-party prescreening of passengers. The announcement sought solutions using "non-governmental data elements to generate an assessment of the risk to the aviation transportation system that may be posed by a specific individual, and to communicate the identity of persons who have successfully passed this risk based assessment to TSA's Secure Flight."[46] In response to clarifying questions on the solicitation, TSA indicated that third parties could make use of any data services that are legally available to them, but noted that data accuracy and security are issues of concern that should be taken into consideration.[47]

The announcement points to the possible future use of large commercial databases to cull information about airline travelers. Given the broad range of commercial data services, this prospect has raised concerns regarding privacy and the accuracy of data that may form the basis of future passenger risk assessments. Historically, such data have primarily been used to assess consumer credit risk and more recently to target marketing and advertising toward specific individuals.

An article published in the *New York Times* in October 2013 raised concerns that passenger prescreening using a wide assortment of non-federal government and private databases may already be taking place, although noting that details of specific programs doing so have not been divulged publicly.[48] The article points specifically to CBP's ATS, although it also identifies Secure Flight, Pre-Check applications, the Pre-Check disqualification list, and TSA's Transportation Security Enforcement Records System (a database of reports and identities tied to violations and potential violations of security regulations) as systems in which commercial data may play a role in risk assessments and where personal information may be used for purposes other than counterterrorism.

Previously, Congress had acted to restrict the use of commercial data in airline passenger prescreening. Specifically, Congress included provisions in appropriations acts during the

[45] Department of Homeland Security, "Privacy Act of 1974; Department of Homeland Security Transportation Security Administration- DHS/TSA-019 Secure Flight System of Records," 78 *Federal Register* 55270-55274, September 10, 2013.

[46] Transportation Security Administration, *Market Research Announcement: TSA Third Part Pre-screening*, HSTS02-13-RFI-0001, January 8, 2013.

[47] Transportation Security Administration, *Market Research Announcement: TSA Third Part Pre-screening*, HSTS02-13-RFI-0001, Amendment 3, February, 6, 2013.

[48] Susan Stellin, "Security Check Now Starts Long Before You Fly," *New York Times*, October 21, 2013.

development and initial deployment of Secure Flight prohibiting the use of data from non-governmental sources to assess the risk of passengers whose names do not appear on government terrorist watchlists.[49] Consequently, congressional oversight and possible legislative action related to TSA systems utilizing commercial data as part of risk-based assessments may be an issue of particular interest as TSA's risk-based approaches to passenger prescreening evolve.

Issues for Congress

Since many of the details regarding TSA's passenger threat assessment and risk-based screening programs cannot be publicly discussed for security reasons, congressional oversight serves an important role in reviewing the various facets of the programs that make up TSA's risk-based approach to airline passenger screening to assure that they are effective and efficient, and provide adequate safeguards for data security and privacy.

In addition to specific concerns raised regarding the use of commercial data in assessing risk and behavioral profiling techniques, TSA's foray into risk-based screening of airline passengers raises a number of broader issues for Congress. Since many of the details regarding TSA's passenger threat assessment and risk-based screening programs cannot be publicly discussed for security reasons, congressional oversight serves an important role in reviewing the various facets of TSA's risk-based approach to airline passenger screening to assure that they are effective and efficient, and provide adequate safeguards for data security and privacy.

One broad concern is the extent to which the various risk-based programs developed by TSA fit into a comprehensive strategy that addresses security risk. As noted above, most experts in the aviation security field do not consider risk-based screening to be a stand-alone technique, but rather to consist of a variety of techniques which, both individually and collectively, fit within a comprehensive risk-based approach to security such as that presented in **Table 1**. There may also be other relevant criteria that would be useful in assessing the degree to which these programs fit into a broader risk-based framework.

An issue of potential significance is the extent to which the risk-based approach, as implemented, is able to effectively adapt and evolve to address shifting threats and to incorporate new methods and capabilities. It is difficult to assess whether the risk-based approach to passenger screening is adequately adaptive and evolving, in part because some elements like the Pre-Check program are relatively new and, in part, because details necessary to make such assessments regarding terrorist watchlists and behavioral profiling techniques are not publicly divulged. The evolution of processes to consolidate and disseminate terrorist watchlist information has been a key issue for the intelligence community since the attempted bombing of Northwest Flight 253 on December 25, 2009. However, specific changes made in response have not been publicly acknowledged. Similarly, information regarding any evolution or adaptation of behavioral detection methods since the inception of TSA's behavioral detection program has not been publicly disclosed. How TSA's risk-based strategy and the underlying intelligence practices informing risk-based decisions have adapted to shifting threat landscapes, potential changes in resources, and the introduction of new procedures and technologies may be an issue of interest for congressional oversight.

[49] See, e.g., P.L. 109-90, §518.

The selection of appropriate metrics appears to be a key issue in assessing the effectiveness of TSA's risk-based strategies. Suitable metrics have been difficult to identify, again, in part because of the necessary secrecy surrounding security. Defining suitable metrics may also prove difficult as a result of relatively limited numbers of encounters with individuals having ties to terrorism, and even fewer still with those seeking to carry out attacks against civil aviation. With regard to behavioral detection programs, TSA's choice of metrics has been questioned. For other programs, such as Pre-Check, TSA has emphasized efficiency metrics rather than metrics that specifically address security effectiveness, at least publicly.

As a practical matter, the limited number of terrorist encounters raises concerns over the prevalence and implications of false alarms, singling out individuals as potential threats who in fact pose no threat. Since the number of suspected terrorists is small relative to the number of airline passengers, false alarms occur with far greater frequency than valid threat detections. Efforts to reduce false positives could leave gaps in threat detection capabilities. Nonetheless, high false alarm rates may lead to potentially significant consequences by misdirecting limited screening resources and by creating complications for individuals mistakenly targeted as potential threats. In the past, initiatives to reduce false alarms associated with Secure Flight have focused on systematic culling and parsing of terrorist databases to ensure that information is thorough, accurate, and up to date. Additionally, a congressionally mandated redress process has been put in place to provide a mechanism for falsely targeted individuals to seek remediation. The effectiveness of these steps in reducing false alarm rates in aviation passenger pre-screening has not been disclosed publicly.

In addition to measuring effectiveness, assessing anticipated efficiency gains related to risk-based screening initiatives appears to have important implications for oversight of TSA operations and appropriations. TSA anticipates that risk-based security efficiencies will result in savings of about $120 million, and allow staffing reductions of more than 1,500 full-time equivalent positions in FY2015.[50] Congressional oversight may examine whether these efficiency gains can be realized without compromising security effectiveness.

Finally, privacy and appropriate data protections are matters of considerable interest to Congress. Through its various systems of records of data maintained on individuals, DHS has established practices to protect personal data and comport with Privacy Act requirements. The extent to which these various privacy protections and data security measures are being appropriately implemented in practice may also be a matter of concern.

In summary, as TSA moves forward in its implementation of a risk-based approach to passenger screening, questions persist as to whether this approach

- appropriately *integrates* various programs and elements of the approach and interdependently and collectively exhibits the characteristics of a *comprehensive risk-based strategy* outlined in **Table 1**;
- adequately *adapts and evolves* to changes in the threat landscape, to potential changes in the availability of resources including personnel, and to the introduction of new procedures and technologies;

[50] Department of Homeland Security, Transportation Security Administration, *Aviation Security: Fiscal Year 2015 Congressional Justification;* Department of Homeland Security, *Budget-in-Brief, Fiscal Year 2015.*

- can identify and analyze *appropriate metrics* for assessing the effectiveness of risk-based programs against specific mission goals tied to detecting and mitigating threats to civil aviation;
- adequately addresses potential *impacts of false positives* without compromising threat detection capabilities; and
- ensures appropriate *privacy and data protections* consistent with those detailed in the agency's SORNs and in a manner that appropriately balances security and intelligence needs with public expectations.

Despite elaborate security measures implemented in the years since the 9/11 terrorist attacks, the potential for a large-scale attack targeting aviation remains. In this context, debate over how to strike a balance between maintaining appropriate levels of privacy while implementing efficient and effective risk-based security strategies to combat terrorism is likely to remain a central issue for aviation security policy and possible congressional oversight.

Author Contact Information

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