The Terrorist Screening Database and Preventing Terrorist Travel

(name redacted)
Specialist in Organized Crime and Terrorism

(name redacted)
Specialist in Aviation Policy

(name redacted)
Specialist in Immigration Policy

November 7, 2016

Summary

After the terrorist attacks of September 11, 2001, the federal government developed a unified regimen to identify and list known or suspected terrorists. The regimen has received repeated congressional attention, and this report briefly discusses for congressional policymakers how the U.S. government fashions and uses the Terrorist Screening Database (TSDB) to achieve such an end. It also discusses how the federal government engages in two travel-related screening processes—visa screening and air passenger screening. Both processes involve subsets of the Terrorist Screening Database.

The Terrorist Screening Database (TSDB)

The TSDB lies at the heart of federal efforts to identify and share information among U.S. law enforcement about identified people who may pose terrorism-related threats to the United States. It is managed by the Terrorist Screening Center (TSC), a multi-agency organization created by presidential directive in 2003 and administered by the Federal Bureau of Investigation (FBI). The TSDB includes biographic identifiers for those known either to have or be suspected of having ties to terrorism. In some instances it also includes biometric information on such people. It stores hundreds of thousands of unique identities. Portions of the TSDB are exported to data systems in federal agencies that perform screening activities such as background checks, reviewing the records of passport and visa applicants, official encounters with travelers at U.S. border crossings, and air passenger screening.

Foreign Nationals Traveling to the United States

Two broad classes of foreign nationals are issued visas under the Immigration and Nationality Act (INA): immigrants and nonimmigrants. Many visitors, however, enter the United States without visas through the Visa Waiver Program (VWP). Under the VWP, foreign nationals from 38 countries with agreements with the United States—including most countries in the European Union—do not need visas to enter the United States for short-term business or tourism and are instead vetted using biographic information to authenticate and screen individuals.

Screening Aliens

Department of State (DOS) consular officers check the background of all visa applicants in "lookout" databases that draw on TSDB information and other counterterrorism information such as the material housed in the National Counterterrorism Center's Terrorist Identities Datamart Environment. DOS specifically uses the Consular Lookout and Support System (CLASS) database, which surpassed 42.5 million records in 2012. Aliens entering through the VWP have been vetted through the Electronic System for Travel Authorization (ESTA), which checks them against the TSDB. In addition, before an international flight bound for the United States departs from a foreign airport, Customs and Border Protection (CBP) officers screen the passenger manifest. CBP inspectors also perform background checks and admissibility reviews at the ports of entry that draw on information from the TSDB.

Screening at the Transportation Security Administration

The Transportation Security Administration (TSA) has initiated a number of risk-based screening initiatives to focus its resources and apply directed measures based on intelligence-driven assessments of security risk. A cornerstone of TSA's risk-based initiatives is the PreCheck program. PreCheck is TSA's latest version of a trusted traveler program that has been modeled

after CBP programs. Under the PreCheck regimen, participants are vetted through a background check process (including screening against terrorist watchlist information). At selected airports, they are processed through expedited screening lanes, where they can keep shoes on and keep liquids and laptops inside carry-on bags.

All passengers flying to or from U.S. airports are vetted using the TSA's Secure Flight program. Secure Flight involves information from the TSDB housed in the No Fly List, Selectee List, and Expanded Selectee List to vet passenger name records. The No Fly List includes identities of individuals who may present a threat to civil aviation and national security. Listed individuals are not allowed to board a commercial aircraft flying into, out of, over, or within U.S. airspace; this also includes point-to-point international flights operated by U.S. carriers. The Selectee List includes individuals who must undergo additional security screening before being allowed to board a commercial aircraft. The Expanded Selectee List was created as an extra security measure in response to a failed attempt to trigger an explosive by a foreign terrorist onboard a U.S.-bound flight on December 25, 2009. It screens against all TSDB records that include a person's first and last name and date of birth that are not already on the No Fly or Selectee lists.

Contents

Figures

Appendixes

Contacts

A fter the terrorist attacks of September 11, 2001, the federal government developed a unified regimen to identify and list known or suspected terrorists. The regimen has received repeated congressional attention, and this report briefly discusses for congressional policymakers how the U.S. government fashions and uses the Terrorist Screening Database (TSDB) to achieve such an end.[1] It also discusses how the federal government engages in two travel-related screening processes—visa screening and air passenger screening. Both processes involve subsets of the Terrorist Screening Database.

The TSDB as well as terrorist watchlisting and screening efforts are of keen congressional interest. This report endeavors to offer policymakers an overview of these issues to help in the development of policy and oversight. The material herein is drawn from publicly available information released by federal agencies as well as other open source material. The report does not evaluate the TSDB or federal programs designed to prevent terrorist travel.

The Terrorist Screening Database

The Terrorist Screening Database (TSDB, commonly referred to as the terrorist watchlist)[2] lies at the heart of federal efforts to collect and share information with U.S. law enforcement and security agencies about identified people who may pose terrorism-related threats to the United States.[3] It is managed by the Terrorist Screening Center (TSC) and includes biographic identifiers for those known either to have or be suspected of having ties to terrorism. In some instances it also includes biometric information on such people.[4] It stores hundreds of thousands of unique identities.[5] Portions of the TSDB are exported to data systems in federal agencies that perform screening activities such as background checks, reviewing the records of passport and visa applicants, and official encounters with travelers at U.S. border crossings.[6]

The Terrorist Screening Center, the Hub of Watchlisting

The TSC, a multi-agency organization administered by the Federal Bureau of Investigation (FBI), maintains the TSDB.[7] The TSC was created by presidential directive in 2003 in response to the terrorist attacks of September 11, 2001.[8] Before the TSC consolidated federal watchlisting efforts,

---

[1] For an example, see U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security, *Safeguarding Privacy and Civil Liberties while Keeping Our Skies Safe*, hearing, 113th Cong., 2nd sess., September 18, 2014.

[2] CRS Report R44529, *The Terrorist Screening Database: Background Information*, by (name redacted)   .

[3] Testimony of Christopher M. Piehota, Director, Terrorist Screening Center, Federal Bureau of Investigation, in U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security, *Safeguarding Privacy and Civil Liberties while Keeping Our Skies Safe*, hearing transcript, 113th Cong., 2nd sess., September 18, 2014 (Hereinafter: Piehota, Testimony).

[4] Testimony of Timothy J. Healy, (former) Director, Terrorist Screening Center, Federal Bureau of Investigation, in U.S. Congress, House Committee on the Judiciary, *Sharing and Analyzing Information to Prevent Terrorism*, hearing transcript, March 24, 2010. Jeremy Scahill, Ryan Devereaux, "Watch Commander: Barak Obama's Secret Terrorist-Tracking System, by the Numbers," *The Intercept,* August 5, 2014 (Hereinafter: Scahill and Devereaux, "Watch Commander").

[5] Department of Justice, Office of Inspector General, "Audit of the Federal Bureau of Investigation's Management of Terrorist Watchlist Nominations," March 2014, footnote 10, p. 2 (Hereinafter: Department of Justice, Office of Inspector General, "Audit").

[6] Ibid. p. 4.

[7] See https://www.fbi.gov/about-us/nsb/tsc/about-the-terrorist-screening-center.

[8] Ibid. The TSC and the TSDB stem from *Homeland Security Presidential Directive/HSPD–6—Directive on* (continued...)

numerous separate watchlists were maintained by different federal agencies. The information in these lists was not necessarily shared or compared.[9]

The efforts that surround the federal watchlisting regimen can be divided into three broad processes centered on the TSDB:

- Nomination, which involves the identification of known or suspected terrorists via intelligence collection or law enforcement investigations. The U.S. government has a formal watchlist nomination process.[10]

- Verification of identities for the TSDB and export of data to screening systems, which involves managing records in the TSDB, as well as the compiling and export of special TSDB subsets for various intelligence or law enforcement end users (screeners).

- Screening, which involves end users—screeners—checking individuals or identities they encounter against information from the TSDB that is exported to screening databases.[11] These databases[12] include the No Fly List and the Selectee and Expanded Selectee lists for airline passenger screening; the Department of State's Consular Lookout and Support System (CLASS); the FBI's National Crime Information Center (NCIC); the TECS (not an acronym) system for border and port of entry screening; and the military base access and screening system. (In FY2011, there were "more than 1.2 billion queries against [the TSDB].")[13] The screening and vetting processes can yield more information on particular subjects that may be fed back into the TSDB.[14]

(See **Figure 1** for a visual depiction of the federal agencies involved in watchlisting.)

(...continued)

Integration and Use of Screening Information to Protect against Terrorism, September 16, 2003. In HSPD-6, the entity described as the Terrorist Threat Integration Center became the TSC.

[9] Federal Bureau of Investigation, "Ten Years After: The FBI since 9/11, Terrorist Screening Center," 2011.

[10] Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015.

[11] Department of Justice, Office of Inspector General, "Audit," p. 1.

[12] For a brief discussion of such databases, see the "Export" and the "National Security and Public Safety Reviews" sections of this report.

[13] Department of Justice, Office of Inspector General, "Audit," p. 2.

[14] For brief descriptions of CLASS and TECS, see "National Security and Public Safety Reviews" and "Export" sections of this report.

Figure 1. U.S. Counterterrorism Watchlisting Regimen
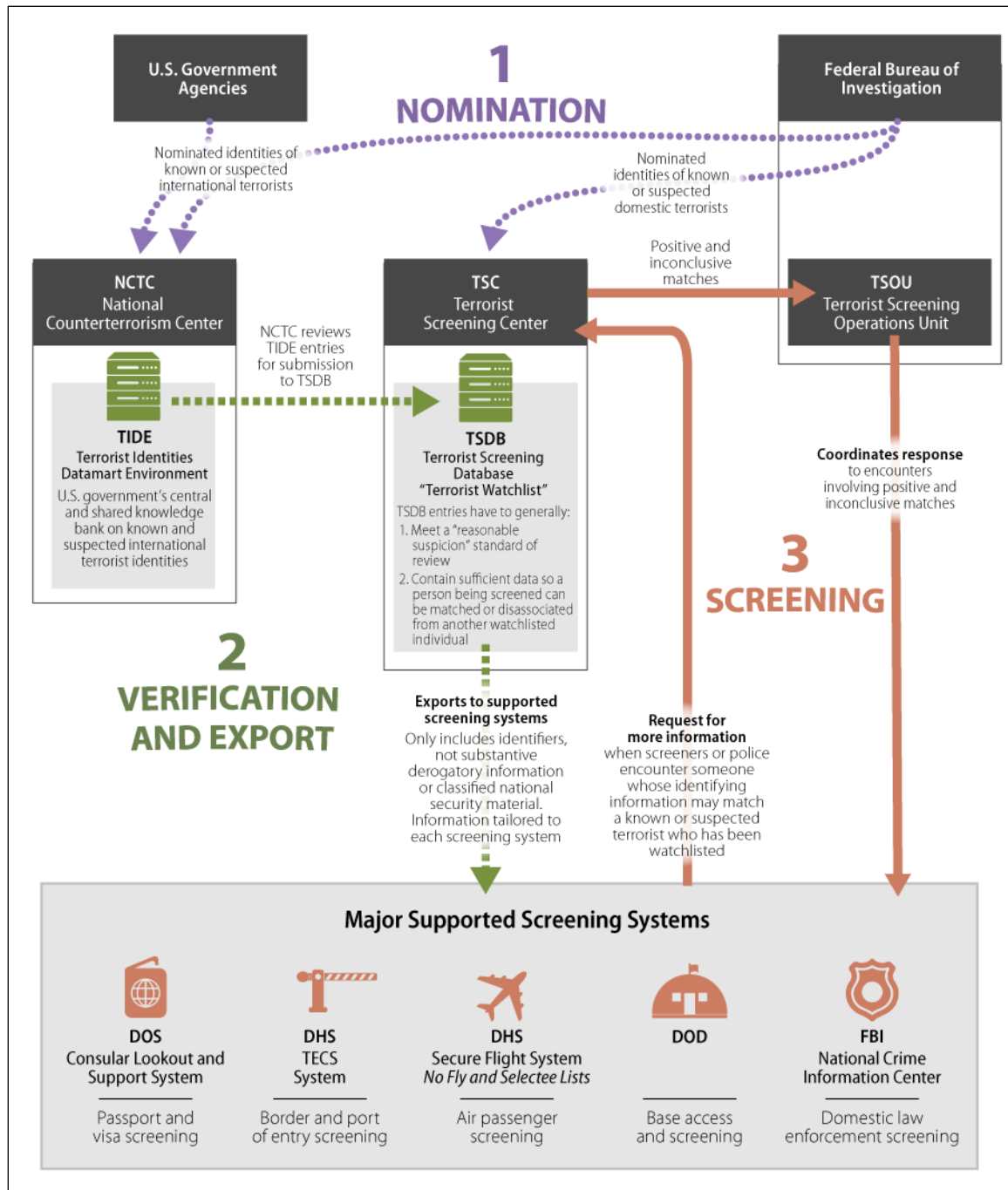
Source: Based on CRS analysis of Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015; Christopher M. Piehota, Director, Terrorist Screening Center, Federal Bureau of Investigation, statement before the House Homeland Security Committee, Subcommittee on Transportation Security, Hearing: "Safeguarding Privacy and Civil Liberties While Keeping our Skies Safe," September 18, 2014; National Counterterrorism Center, "Terrorist Identities Datamart Environment (TIDE)," August 1, 2014; Department of Justice, Office of Inspector General, "Audit of the Federal Bureau of Investigation's Management of Terrorist Watchlist Nominations," March 2014.

Nominations

The first step toward adding identities to the TSDB is the nomination process. In their daily work poring over raw information or case files, staff at U.S. government agencies—dubbed "originators" in the watchlisting process—uncover the possible identities of people suspected of involvement in terrorist activity. Such identities can be nominated for addition to the TSDB. Originators can work in places such as intelligence and law enforcement agencies or U.S embassies and consulates. The nominations they initiate include people who are classed together in the watchlisting regimen as "known or suspected terrorists" (KSTs).

For the federal government's watchlisting regimen, a "known terrorist" is

> an individual whom the U.S. government knows is engaged, has been engaged, or who intends to engage in terrorism and/or terrorist activity, including an individual (a) who has been charged, arrested, indicted, or convicted for a crime related to terrorism by U.S. government or foreign government authorities; or (b) identified as a terrorist or member of a designated foreign terrorist organization pursuant to statute, Executive Order, or international legal obligation pursuant to a United Nations Security Council Resolution.[15]

A "suspected terrorist" is

> an individual who is reasonably suspected to be, or has been, engaged in conduct constituting, in preparation for, in aid of, or related to terrorism and/or terrorist activities based on an articulable and reasonable suspicion.[16]

Verification of Identities for the TSDB and Export to Federal Data Systems

All nominated identities of known or suspected terrorists for the TSDB are vetted by analysts at either the National Counterterrorism Center (NCTC) or the FBI and then undergo verification at the TSC.[17]

NCTC handles the nominations of all known or suspected international terrorists (including purely international suspects submitted by the FBI). In this process, NCTC maintains a classified database known as the Terrorist Identities Datamart Environment (TIDE). TIDE is the U.S. government's "central repository of information on international terrorist identities."[18] TIDE includes:

> to the extent permitted by law, all information the [U.S. government] possesses related to the identities of individuals known or appropriately suspected to be or to have been

---

[15] Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015. See also Piehota, Testimony.

[16] Ibid.

[17] Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015; Department of Justice, Office of Inspector General, "Audit," p. 3. The nomination process is governed by watchlist procedures described in "Watchlisting Guidance" developed by the "watchlisting community." The community includes the Office of the Director of National Intelligence, the Central Intelligence Agency, the National Geospatial Intelligence Agency, the National Security Agency, the National Reconnaissance Office, the Department of Justice, the Department of Defense, the Department of State, the Department of the Treasury, the Department of Homeland Security, and the Department of Energy.

[18] TIDE is the "central and shared knowledge bank on known and suspected terrorists and international terror groups" mandated by the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). See National Counterterrorism Center, "Terrorist Identities Datamart Environment (TIDE)," August 1, 2014.

---

involved in activities constituting, in preparation for, in aid of, or related to terrorism (with the exception of purely domestic terrorism information).[19]

In late 2013, TIDE contained the identities of approximately 1.1 million people. Of this number, about 25,000 were U.S. citizens and lawful permanent residents[20] linked to international terrorist organizations.[21] Not all of the entries in TIDE get into the TSDB, which according to the FBI held approximately 800,000 identities in November 2014.[22] NCTC analysts constantly work on updating identities in TIDE, and NCTC exports a subset of its TIDE data holdings for the TSDB.[23] TSC analysts perform a final verification of identities before they become a part of the TSDB. (For more about the concepts involved, see "Making the TSDB Cut.") TIDE is also an important resource on its own, used by counterterrorism professionals throughout the U.S. intelligence community[24] in daily counterterrorism analytical work.

FBI analysts in its Terrorist Review and Examination Unit process FBI nominations to the TSDB.[25] These nominations often spring from FBI investigative work. The unit forwards international nominations to NCTC for inclusion in TIDE, where the data in the nomination is reviewed before release to the TSC.[26] The FBI also forwards nominations of purely domestic terrorists and "domestic terrorists that may have connections to international terrorism" *directly to* the TSC for review.[27]

Making the TSDB Cut

To make it into the TSDB, a nomination vetted by either NCTC or the FBI has to (1) meet the "reasonable suspicion watchlisting standard" *and* (2) have sufficient identifiers. TSC personnel verify that each nomination that makes it into the TSDB meets both of these criteria.[28] The TSDB is a sensitive but unclassified dataset, and each record created by TSC personnel for the TSDB includes only an individual's identifiers and no "substantive derogatory information or classified national security" material.[29]

Reasonable Suspicion

Articulable facts form the building blocks of the reasonable suspicion standard undergirding the nomination of suspected terrorists. Sometimes the facts involved in identifying an individual as a possible terrorist are not enough on their own to develop a solid foundation for a nomination. In

---

[19] Ibid.

[20] A lawful permanent resident (LPR) refers to a foreign national who has been admitted to the United States to live and work indefinitely. It is synonymous with immigrant or legal permanent resident.

[21] Ibid.

[22] U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security, *Safeguarding Privacy and Civil Liberties while Keeping Our Skies Safe*, hearing transcript, 113th Cong., 2nd sess., September 18, 2014, p. 25. In 2013, there were 700,000. Also see Jeremy Scahill, Ryan Devereaux, "Watch Commander: Barak Obama's Secret Terrorist-Tracking System, by the Numbers," *The Intercept,* August 5, 2014 (Hereinafter: Scahill and Devereaux, "Watch Commander").

[23] Ibid.

[24] For a description, see http://www.dni.gov/index.php.

[25] Department of Justice, Office of Inspector General, "Audit," pp. 3-8.

[26] Ibid, p. 9.

[27] Piehota, Testimony.

[28] Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015.

[29] Piehota, Testimony.

such cases, investigators and intelligence analysts make rational inferences regarding potential nominees.[30] The TSC vets all nominations, and when it concludes that the facts, bound with rational inferences, hold together to form a reasonable determination that the person is suspected of having ties to terrorist activity, the person is included in the TSDB.[31] In the nomination process, guesses or hunches alone are not supposed to lead to reasonable suspicion. Likewise, one is not supposed to be designated a known or suspected terrorist based solely on activity protected by the First Amendment or race, ethnicity, national origin, and religious affiliation.[32]

Identifiers

Once the reasonable suspicion standard is met, analysts must have the ability to distinguish a specific terrorist's identity from others. Thus, minimum biographic criteria must exist. At the very least, for inclusion in the TSDB a record must have a last name "and at least one additional piece of identifying information (for example a first name or date of birth)."[33]

Most nominations appear to make the TSDB cut. From FY2009 to FY2013, approximately 1.6 million individuals were nominated and only about 1% (just over 14,000) were rejected. (See **Figure 2**.)

---

[30] Exceptions to the reasonable suspicion threshold exist, and some people are placed in the TSDB "to support immigration and border screening by the Department of State and the Department of Homeland Security." See Piehota, Testimony. Presumably, an example of this was the reported watchlisting of the father of one of the shooters implicated in the San Bernardino shooting incident in December 2015. See also Paula Mejia, "Here's How You End up on the U.S. Watchlist for Terrorists," *Newsweek*, July 25, 2014. The FBI "generally requires" that subjects of closed terrorism investigations be removed from the TSDB. Limited exceptions exist. Department of Justice, Office of Inspector General, "Audit," p. 10.

[31] This means that the individual is suspected of engaging in conduct constituting, preparing for, aiding in, or related to terrorism and/or terrorist activities.

[32] There are "limited exceptions to the reasonable suspicion requirement, which exist to support immigration and border screening by the Department of State and Department of Homeland Security." See Piehota, Testimony.

[33] Department of Justice, Office of Inspector General, "Audit," p. 3.

Figure 2. Nominations and Rejections to Terrorist Screening Database,
FY2009-FY2013
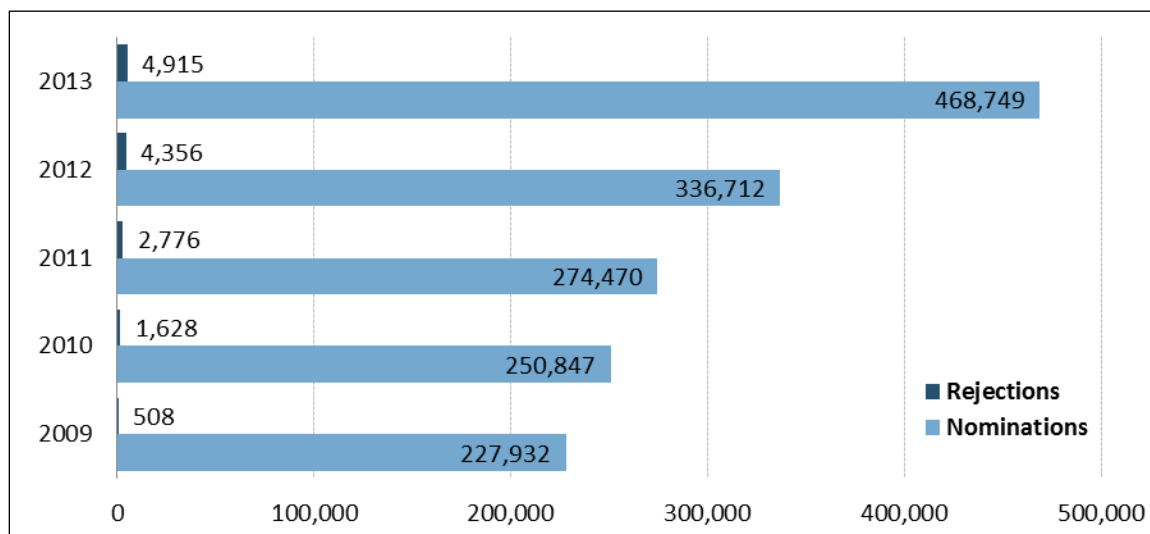
Source: CRS presentation of information from *Gulet Mohamed v. Eric Holder et al.*, "Defendant's Objections and Responses to Plaintiff's First Set of Interrogatories," U.S. District Court, Eastern District of Virginia, April 7, 2014.

Notes: In total, 1,558,710 nominations were made from FY2009 to FY2013; 14,183 were rejected (0.9%).

Export

The TSC routinely exports watchlist information to federal agencies authorized to conduct terrorist screening. According to the TSC, this occurs as the information is processed: "seconds later, it shows up with our partners so they can do near-real-time screening."[34] According to the TSC, those partners consist of "five major U.S. Government agencies" that receive TSDB exports, which are subsets of the entire watchlist.[35] Each of the agencies gets a different portion of the TSDB that is "tailored to [its] mission, legal authorities, and information technology requirements."[36] Among the agencies whose screening systems make use of TSDB information are the following:

The **Department of State's** (DOS's) consular officers draw on TSDB information in the Consular Lookout and Support System (CLASS) used for passport and visa screening.

The **Transportation Security Administration** (TSA) uses information from the TSDB for aviation security screening. The No Fly List, the Selectee List, and the Expanded Selectee List are compared to passenger records using a program known as Secure Flight. The No Fly List includes identities of individuals who may present a threat to civil aviation and national security. Listed individuals are not allowed to board a commercial aircraft "flying into, out of, over, or within United States airspace; this also includes point-to-point international flights operated by U.S.

---

[34] U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security, *Safeguarding Privacy and Civil Liberties while Keeping Our Skies Safe*, hearing transcript, 113th Cong., 2nd sess., September 18, 2014, p. 24.

[35] Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015; Department of Justice, Office of Inspector General, "Audit," p. 9.

[36] Piehota, Testimony.

carriers."[37] (As discussed below, Customs and Border Protection [CBP] screens the passenger manifest before any international flight is allowed to depart to the United States.) The Selectee List includes individuals who must undergo additional security screening before being allowed to board a commercial aircraft. The minimum derogatory information requirements that form the basis for including an identity in the No Fly List and the Selectee List are "more stringent than the TSDB's known or reasonably suspected standard,"[38] although the specific criteria for inclusion on these lists are not publicly disclosed. The stricter criteria make these lists much smaller than the TSDB. In 2014, there were approximately 800,000 identities in the TSDB according to the FBI, roughly double the figure reported in 2008.[39] By comparison, in 2014 only about 8% of the TSDB identities—around 64,000—were on the No Fly List, and about 3%—roughly 24,000—were on the Selectee List.[40]

The Expanded Selectee List, an extra security measure developed in response to a failed attempt to trigger an explosive by a foreign terrorist onboard a U.S.-bound flight on December 25, 2009, screens against all TSDB records that include a person's first and last name and date of birth that are not already on the No Fly or Selectee lists.[41] This may be used at times of heightened terrorism threats, although TSA has not publicly explained when it relies on the Expanded Selectee List as opposed to the standard Selectee List to identify passengers for enhanced airport checkpoint screening.

Customs and Border Protection (CBP) owns and uses TECS (not an acronym), the main system that CBP officers employ at the border and elsewhere to screen arriving travelers and determine their admissibility.[42] TECS accepts "nearly all" records from the TSDB.[43] CBP also uses the Automated Targeting System (ATS), which is "a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments."[44] As one of its functions, ATS "compares information about travelers and cargo arriving in, transiting through, or exiting the country, against law enforcement and intelligence databases" including information from the TSDB.[45] As its name suggests, Automated Targeting System-Passenger (ATS-P) is the portion of

---

[37] See Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015.

[38] Department of Homeland Security, Office of Inspector General, *Role of the No-Fly and Selectee Lists in Securing Commercial Aviation,* (redacted), July 2009, p. 9.

[39] U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security, *Safeguarding Privacy and Civil Liberties while Keeping Our Skies Safe*, hearing transcript, 113th Cong., 2nd sess., September 18, 2014, p. 25. According to media reporting, in 2013 there were about 700,000 people on the watchlist. See Scahill and Devereaux, "Watch Commander." See also Rick Kopel, (then) Principal Deputy Director, Terrorist Screening Center, Federal Bureau of Investigation, written statement before the House Homeland Security Committee, Subcommittee on Transportation Security and Infrastructure Protection, September 9, 2008.

[40] Piehota, Testimony.

[41] The Expanded Selectee List is not an official subset of the TSDB, however. See Department of Homeland Security Office of Inspector General, *Implementation and Coordination of TSA's Secure Flight Program,* (redacted), July 2012, p. 6; U.S. Government Accountability Office, *Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness*, GAO-14-531, September 2014, p. 14 (Hereinafter: Government Accountability Office, *Secure Flight*).

[42] Department of Homeland Security, Office of Inspector General, *Role of the No-Fly and Selectee Lists in Securing Commercial Aviation,* (redacted), July 2009, p. 14.

[43] Department of Homeland Security, Office of Inspector General, *Implementation and Coordination of TSA's Secure Flight Program,* (redacted), July 2012, p. 6.

[44] Department of Homeland Security, *Automated Targeting System—TSA/CBO Common Operating Picture, Phase II,* Privacy Impact Assessment Update, September 16, 2014, p. 1.

[45] Ibid.

ATS focused on passengers, "for the identification of potential terrorists, transnational criminals, and, in some cases, other persons who pose a higher risk of violating U.S. law"[46] and is used by CBP personnel at the border, ports of entry, and elsewhere, including screening the passenger manifests of all U.S. bound international flights.[47]

The **FBI** runs the National Crime Information Center's (NCIC's) database, which it has described as "an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year."[51] The NCIC includes 21 files. One of them, the "Known or Appropriately Suspected Terrorist File" includes TSDB records. The NCIC database is used for domestic law enforcement screening.[52]

The **Department of Defense** uses TSDB information to help screen people trying to enter military bases.[53]

> ## Rules-Based Screening—Looking for Potential Threats without Relying on Identities
>
> The federal government is not aware of all the identities of people with ties to terrorist groups who may threaten the United States. Thus, a watchlisting regimen founded on identities is inherently incomplete. In a push for a more complete sense of threat, CBP and TSA have established systems that assess the risk of particular travelers based on rules—"patterns identified as requiring additional scrutiny."[48] CBP's ATS includes such rules. CBP establishes "rules" for ATS "based on CBP officer experience, analysis of trends of suspicious activity, law enforcement cases and raw intelligence" and looks for travelers or cargo hewing to such patterns.[49] Additionally, TSA works with CBP data and also establishes its own rules based on intelligence analysis to create two watchlists within TSA's Secure Flight Program. These have not been publicly named.[50]

Screening

Employees from U.S. federal, state, and local law enforcement agencies who perform screening activities (screeners) check the identities of individuals they encounter in their daily work against specific subsets of the TSDB. Such queries happen either in-person or via submitted official (electronic or paper) forms. Examples include instances when

- foreign visitors and returning U.S. citizens enter the United States at a port of entry and are screened by CBP officers;
- state or local police pull over vehicles for moving violations and interact with drivers and passengers; and

---

[46] Department of Homeland Security, *Automated Targeting System,* Privacy Impact Assessment, June 1, 2012, p. 6.

[47] Department of Homeland Security, *Automated Targeting System—TSA/CBO Common Operating Picture, Phase II,* Privacy Impact Assessment Update, September 16, 2014, p. 1.

[48] Ibid., p. 2.

[49] Ibid.

[50] Government Accountability Office, *Secure Flight*, pp. 12-13.

[51] See https://www.fbi.gov/about-us/cjis/ncic. The FBI describes how NCIC is used by noting that "criminal justice agencies enter records into NCIC that are accessible to law enforcement agencies nationwide. For example, a law enforcement officer can search NCIC during a traffic stop to determine if the vehicle in question is stolen or if the driver is wanted by law enforcement. The system responds instantly. However, a positive response from NCIC is not probable cause for an officer to take action. NCIC policy requires the inquiring agency to make contact with the entering agency to verify the information is accurate and up-to-date. Once the record is confirmed, the inquiring agency may take action to arrest a fugitive, return a missing person, charge a subject with violation of a protection order, or recover stolen property."

[52] Ibid. Also see Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015.

[53] Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015. TSDB information is also shared with some foreign allies.

- foreign applicants submit visa applications that are reviewed by Department of State officials.[54]

Every year, more than 1 billion queries are likely made against information in the TSDB.[55] Queries that yield possible matches between the identifying information provided by individuals and TSDB holdings are known as "encounters."[56] Screeners receive notification of possible matches via their specific screening databases.[57]

When a query produces an encounter, screeners are directed to contact the TSC. Employees in the TSC's 24-hour operations center perform additional research to track down any information that "may assist in making a conclusive identification."[58] (Screeners have access only to the identifying information available in the TSDB, while TSC analysts can search through additional datasets and intelligence to clarify a possible match.) If a positive match is made or if the TSC analysis is inconclusive, the FBI's Terrorist Screening Operations Unit coordinates how the government responds; "For example, [the unit] may deploy agents to interview and possibly apprehend the subject."[59] Any new information collected from an encounter is forwarded to the TSC to enhance any related existing TSDB entry.[60]

Visa and Air Traveler Screening

The use of TSDB information by federal agencies to thwart the international movement of terrorists is highlighted in efforts to screen foreigners who apply for U.S. visas and those who enter via the Visa Waiver Program (VWP), and in the general screening of air travelers.[61] In these instances, information from the TSDB helps to keep terrorists from using legitimate means of visitation and travel to find harbor in the United States.

Overview of the Visa Screening Process

Immigration Law and Terrorism

Engaging in specified terrorist activity, as well as a broad range of activities in support of terrorism, generally bars the entry of a foreign national into the United States. The Immigration and Nationality Act (INA) expressly provides that aliens who have engaged or intend to engage in terrorist activity—either as an individual or as a member of a terrorist organization—are inadmissible. The INA allows the categorizations of individuals and groups as terrorists in a process that is distinct from diplomatic, foreign policy, or military policy considerations. The terror-related activities that would prevent someone from immigrating to the United States are

---

[54] Examples suggested in Department of Justice, Office of Inspector General, "Audit," p. 1.

[55] Ibid, p. 2.

[56] Ibid.

[57] Department of Justice, Office of Inspector General, "Audit," p. 4.

[58] Ibid., pp. 4-5.

[59] Ibid., p. 5.

[60] Ibid. People seeking to have their names removed from the TSDB because of "difficulties experienced during travel screening at transportation hubs, such as airports, seaports, train stations, or U.S. border crossings" can use DHS's Traveler Redress Inquiry Program (DHS TRIP). See Federal Bureau of Investigation, "Terrorist Screening Center: Frequently Asked Questions," September 25, 2015. For more information on DHS TRIP, see https://www.dhs.gov/dhs-trip. See also the "Air Passenger Risk-Based Screening" section in this report.

[61] For information on the VWP, see CRS Report RL32221, *Visa Waiver Program*, by (name redacted)

applicable whether or not they are directed against the United States, and whether or not the foreign national's admission would pose a threat to U.S. security.

The statutory language permitting the exclusion of aliens on the basis of membership in organizations deemed subversive to national security dates back to the Immigration Act of March 3, 1903.[62] The Alien Registration Act of 1940 made past and current membership in proscribed organizations and subversive classes of aliens additional grounds for exclusion. When the various immigration and citizenship laws were unified and codified as the Immigration and Nationality Act of 1952 (INA),[63] the result was three separate grounds for exclusion that pertained to national security or political subversives.[64] The Immigration Amendments Act of 1990[65] streamlined and modernized the security, foreign policy, and political grounds for exclusion, and added a terrorism-related ground of exclusion to the INA. In part as a response to the 1993 World Trade Center bombing, Congress strengthened the anti-terrorism provisions in the INA through the Illegal Immigration Reform and Immigrant Responsibility Act[66] and the Antiterrorism and Effective Death Penalty Act.[67] The USA PATRIOT Act of 2001 and the REAL ID Act of 2005[68] continued the trend to expand the national security-related grounds for exclusion.[69]

There are two broad classes of foreign nationals that are issued visas:

- *Immigrants*, foreign nationals who wish to come to live permanently in the United States and are issued immigrant visas, and

- *Nonimmigrants*, foreign nationals who seek to come to the United States temporarily and are issued nonimmigrant visas.[70]

A visa applicant is required to submit his or her photograph and fingerprints, as well as full name (and any other name used or by which he or she has been known), age, gender, and the date and place of birth. Depending on the visa category, certain documents must be certified by the proper government authorities (e.g., birth certificates and marriage licenses). All prospective lawful permanent residents must submit to physical and mental examinations, and prospective nonimmigrants also may be required to have physical and mental examinations. These reviews

---

[62] Even though the statutory definitions have been revised over time, for the purposes of this report the terms "excludeable" and "inadmissible" are used interchangeably, as are "exclusion" and "inadmissibility." In both instances, the meanings center on the basis for denying a visa or denying admission to the United States.

[63] Also known as the McCarran-Walter Act, P.L. 82-414.

[64] The Immigration and Nationality Act, which was passed as the McCarran-Walter Act of 1952, added 9 new grounds for exclusion along with 22 grounds that were in current law at that time. When President Harry Truman vetoed the McCarran-Walter Act, he specifically criticized the national security-related grounds. Congress successfully overrode his veto, and he signed the Immigration and Nationality Act on June 17, 1952 (66 Stat. 163).

[65] P.L. 101-649.

[66] P.L. 104-208.

[67] P.L. 104-132.

[68] P.L. 107-56 and P.L. 109-13.

[69] CRS Report RL32564, *Immigration: Terrorist Grounds for Exclusion and Removal of Aliens*, by (name redacted) and (name redacted)   .

[70] Humanitarian admissions, such as asylees, refugees, parolees, and other aliens granted relief from deportation, are handled separately under the Immigration and Nationality Act (INA). Persons granted asylum or refugee status are ultimately eligible to become lawful permanent residents. For more on refugees, see CRS Report RL31269, *Refugee Admissions and Resettlement Policy*, by (name redacted). Illegal aliens or unauthorized aliens include those noncitizens who entered the United States without an official inspection at a port of entry, entered with fraudulent documents, or violated the terms of their visas after entering the United States. For more, see CRS Report R43892, *Alien Removals and Returns: Overview and Trends*, by (name redacted)

are intended to ensure that aliens are not ineligible for visas or admission under the INA Section 212(a) grounds for inadmissibility.[71]

Many visitors, however, enter the United States without nonimmigrant visas through the VWP.[72] This provision of the INA allows the Attorney General to waive the visa documentary requirements for aliens coming as visitors from 38 countries. Aliens entering through the VWP have been vetted through a system, known as the Electronic System for Travel Authorization (ESTA), that checks them against the TSDB.[73] (See "National Security and Public Safety Reviews" below.) As with all foreign nationals, CBP inspectors at the port of entry perform background checks and admissibility reviews that draw on information from the TSDB. (See "Export" and "Screening" above.)

National Security and Public Safety Reviews

For some years, consular officers have been required to check the background *of all visa applicants* in the "lookout" databases and part of that process involves screening against information from the TSDB.[74]

The Department of State (DOS) specifically uses the Consular Lookout and Support System (CLASS) database, which surpassed 42.5 million records in 2012 and contains a subset of the TSDB. (See "Export" and "Screening" above.) Consular officers use name-searching algorithms to ensure matches between names of visa applicants and any derogatory information contained in CLASS. DOS reports that about 70% of the records in CLASS come from other agencies, including the Department of Homeland Security (DHS), the FBI, and the Drug Enforcement Administration. DOS also employs an automated CLASS search algorithm that runs the names of all visa applicants against the Consular Consolidated Database (CCD) to check for any prior visa applications, refusals, or issuances.[75] The CCD is a biometric and biographic database encompassing all visa applicants. Since February 2001, the CCD has stored photographs of all visa applicants in electronic form; since 2007, the CCD has stored 10-finger scans.[76] The digital photograph and the 10-finger electronic scan are the standard for biometric data collected by U.S. embassies and consulates.

DOS has relied on the Security Advisory Opinion (SAO) system, which requires a consular officer abroad to refer selected visa cases for greater review by intelligence and law enforcement

---

[71] The grounds of inadmissibility under INA §212(a) include health-related grounds, criminal history, security and terrorist concerns, public charge (e.g., indigence), seeking to work without proper labor certification, illegal entrants and immigration law violations, ineligibility for citizenship, and aliens who are illegally present or have previously been removed.

[72] CRS Report RL32221, *Visa Waiver Program*, by (name redacted)

[73] P.L. 110-53 required DHS to implement an electronic travel authorization system and other enhancements to the VWP, and DHS established ESTA so that those traveling under the VWP would undergo a security screening before traveling to the United States. Travelers under the VWP may not travel to the United States without an approval from ESTA.

[74] Lookout databases store information on persons whose entry might pose a threat to the safety or security of the United States.

[75] Testimony of David T. Donahue, Deputy Assistant Secretary for Visa Services, in U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *From the 9/11 Hijackers to Amine El-Khalifi: Terrorists and the Visa Overstay Problem*, 112th Cong., 2nd sess., March 6, 2012.

[76] Consular officers transmit the fingerprints taken during the visa process to CBP officers at ports of entry, enabling them to match the fingerprints of persons entering the United States.

agencies.[77] The current interagency procedures for alerting officials about foreign nationals who may be suspected terrorists, referred to in DOS nomenclature as Visa Viper, began after the 1993 World Trade Center bombing and were institutionalized by enactment of the Enhanced Border Security and Visa Entry Reform Act of 2002. If consular officials receive information about a foreign national that causes concern, they send a Visa Viper cable (which is a dedicated and secure communication) to the National Counterterrorism Center (NCTC).

In a similar set of SAO procedures, consular officers send suspect names, identified by law enforcement and intelligence information, to the FBI for a name check program called Visa Condor.[78] There is also the "Terrorist Exclusion List," which lists organizations designated as terrorist-supporting and includes the names of individuals associated with these organizations.[79]

In June 2013, DOS launched an initiative known as "Kingfisher Expansion" (KFE) in partnership with the NCTC for conducting interagency counterterrorism screening of all visa applicants.[80] Under KFE protocols, the consular official submits the visa applicants' electronic visa applications as a "vetting package" to the NCTC. In turn, the NCTC uses an automated process to compare the vetting package with its holdings, most notably the Terrorist Identities Datamart Environment (TIDE) on known and suspected terrorists and terrorist groups. (For a brief discussion of TIDE, see "Verification of Identities for the TSDB and Export to Federal Data Systems" above.) A hit in KFE triggers a Washington-based interagency review of the visa application. KFE also conducts post-issuance reviews of valid visas to check for new information on emerging threats.[81]

Despite dipping somewhat in FY2013, the number of aliens denied nonimmigrant visas under terrorist grounds of inadmissibility has increased since the 1990s and mid-2000s. FY2012 was the peak year for immigrant denials based on national security grounds. As **Figure 3** shows, the general trends hold for immigrant and nonimmigrant exclusions.[82]

What about travelers from Visa Waiver Program (VWP) countries where their citizens do not need visas to travel to the United States?[83] In implementing the VWP, CBP uses the Electronic System for Travel Authorization (ESTA), a security vetting tool, to review prospective travelers from visa waiver countries "to determine if they pose a law enforcement or security risk before they board aircraft destined for the United States."[84] ESTA draws on records from the TSBD.

---

[77] U.S. Congress, Senate Committee on Foreign Relations, Subcommittee on International Operations and Terrorism, *The Post 9/11 Visa Reforms and New Technology: Achieving the Necessary Security Improvements in a Global Environment*, hearing, October 23, 2003.

[78] Ibid.

[79] For further discussion of terrorist screening, see CRS Report RL32564, *Immigration: Terrorist Grounds for Exclusion and Removal of Aliens*, by (name redacted) and (name redacted)   .

[80] KFE also coordinates with DHS (including CBP and U.S. Immigration and Customs Enforcement (ICE)), the FBI, and the FBI's Terrorist Screening Center.

[81] Testimony of Edward J. Ramotowski, Deputy Assistant Secretary for Visa Services, in U.S. Congress, House Committee on Oversight and Government Reform, Subcommittee on National Security, *Hearing on Securing the U.S. Border, B1/B2 Visas and Border Crossing Cards*, 113th Cong., 1st sess., November 14, 2013.

[82] Bureau of Consular Affairs, *Report of the Visa Office*, U.S. Department of State, Table XX (multiple years).

[83] See http://www.cbp.gov/travel/international-visitors/visa-waiver-program/visa-waiver-program-improvement-and-terrorist-travel-prevention-act-faq. For background on the Visa Waiver Program, see CRS Report RL32221, *Visa Waiver Program*, by (name redacted)

[84] For details see Customs and Border Protection, "Strengthening Security of the VWP through Enhancements to ESTA," press release.

In November 2014, DHS responded to concerns regarding terrorists entering the United States from VWP countries by expanding the information collected from VWP travelers through ESTA.[85] DHS has stated that ESTA has been a "highly effective security and vetting tool" enabling "DHS to deny travel under the VWP to thousands of prospective travelers who may pose a risk to the United States [presumably endangering national security or public safety], prior to those individuals boarding a U.S. bound aircraft."[86] However, since ESTA is a biographic and not a biometric security check and there is no interview by a consular officer, some contend that ESTA does not provide the same level of screening as a visa application.[87]

In addition to the enhancements of ESTA data elements discussed above, in 2015 DHS boosted the security criteria that countries "must meet to participate in the VWP."[88] Also, in December 2015 Congress passed legislation requiring changes to the VWP.[89] Among other changes, the legislation established new eligibility requirements for the VWP which, as implemented, modified what data were to be collected from travelers via ESTA.[90] Furthermore, as of April 2016 all foreign travelers participating in the VWP have to use e-Passports.[91]

---

[85] P.L. 110-53. Department of Homeland Security, Customs and Border Protection, "ESTA - New questions to the ESTA application," CBP INFO Center, Washington, DC, November 3, 2014, https://help.cbp.gov/app/answers/detail/a_id/1756/~/esta—new-questions-to-the-esta-application.

[86] Testimony of Francis Taylor, Under Secretary for Intelligence and Analysis, Department of Homeland Security, in U.S. Congress, House Committee on Homeland Security, *Terrorism Gone Viral: The Attack in Garland, Texas and Beyond,* 114th Cong., 1st Sess., June 3, 2015.

[87] See CRS Report RL32221, *Visa Waiver Program*, by (name redacted)

[88] Department of Homeland Security, "Statement by Secretary Jeh C. Johnson on House Homeland Security Committee Task Force Report on Combating Terrorist and Foreign Fighter Travel," press release, September 30, 2015 (Hereinafter: Johnson, "Statement on House Homeland Security").

[89] See Consolidated Appropriations Act, 2016 (P.L. 114-113; H.R. 2029). For a discussion of the VWP provisions in the bill, see "Legislation in the 114th Congress," in CRS Report RL32221, *Visa Waiver Program*, by (name redacted)

[90] Certain travelers are no longer eligible to travel or be admitted to the United States under the VWP. These include (1) nationals of VWP countries who have been present in Iraq, Syria, countries listed under specified designation lists, or countries deemed appropriate by the DHS Secretary (currently including Iran, Libya, Somalia, Sudan, and Yemen) at any time on or after March 1, 2011 (there are limited exceptions); and (2) nationals of VWP countries who are also nationals of Iraq, Syria, Iran, or Sudan. Travelers who fall under these restrictions are not barred from entering the United States, but they must obtain a visa from a U.S. Embassy or Consulate for such travel. See http://www.cbp.gov/travel/international-visitors/visa-waiver-program/visa-waiver-program-improvement-and-terrorist-travel-prevention-act-faq.

[91] Such passports include "the security feature of an electronic chip, which holds all of a passenger's information including name, date of birth and other biographical information. This not only protects privacy and prevents identity theft, but also helps to safely identify a passenger, making travel safer and faster." See Department of Homeland Security, "Statement by Secretary Jeh C. Johnson on Strengthening Travel Security with E-Passports," press release, April 1, 2016.

Figure 3. Foreign Nationals Denied Visas under Terrorist Grounds of Inadmissibility

FY2000-FY2015
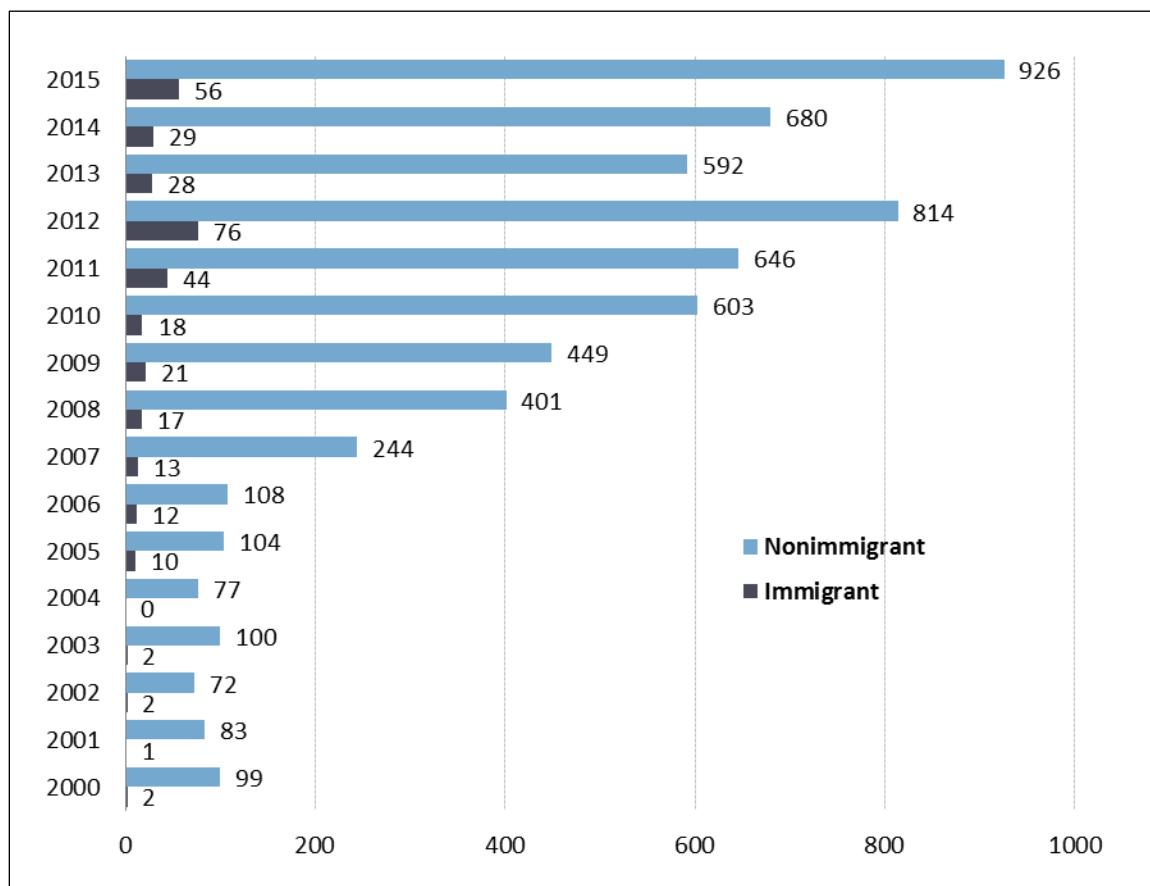
Source: CRS presentation of initial determination data from Table XX of the annual reports of the U.S. Department of State, Office of Visa Statistics (multiple years).

Notes: Data are initial determinations of inadmissibility. Some denials may be overcome with additional evidence. In 2000, the Department of State (DOS) issued 413,521 immigrant visas and 7.6 million nonimmigrant visas. In FY2015, DOS issued 531,463 immigrant visas, and 10.9 million nonimmigrant visas. Table I of the annual reports of the U.S. Department of State, Office of Visa Statistics (multiple years).

Air Passenger Risk-Based Screening

TSA has initiated a number of risk-based passenger screening initiatives to focus its resources and apply directed measures based on intelligence-driven assessments of security risk. These efforts involve identifying known threats to aviation by comparing passenger names and birthdates to the No Fly and Selectee lists, and potentially the Expanded Selectee List, to deny boarding to No Fly matches and apply enhanced screening processes to Selectees. It also involves identifying low-risk travelers who can be routinely granted expedited physical screening so that TSA screening resources can be focused on passengers of unknown risk that TSA has no information about and on passengers that pose an elevated risk (i.e., Selectees).

Identifying Low-Risk Travelers

In 2001, the Aviation and Transportation Security Act (P.L. 107-71) authorized TSA to "establish requirements to implement trusted passenger programs and use available technologies to expedite

the security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening."

A cornerstone of TSA's risk-based initiatives created under this authority is the PreCheck program. PreCheck is TSA's latest version of a trusted traveler program.[92] Under PreCheck, participants vetted through a background check process (including screening against terrorist watchlist information) are processed through expedited screening lanes where they can keep shoes on and keep liquids and laptops inside carry-on bags. As of May 2016, PreCheck expedited screening lanes were available at more than 150 airports. The cost of background checks under the PreCheck program is recovered through application fees of $85 per passenger for a five-year membership. TSA's goal is to process 50% of passengers through PreCheck expedited screening lanes, thus reducing the need for standard security screening lanes.

A predecessor test program called the Registered Traveler program, which involved private vendors that issued and scanned participants' biometric credentials, was scrapped by TSA in 2009 because it failed to show a demonstrable security benefit. However, PreCheck has demonstrated improved screening efficiency, resulting in cost savings for TSA. TSA estimates annual savings in screener workforce costs totaling $110 million as a result of risk-based screening efficiencies.[93] Provisions in the FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) included language to expand the PreCheck program by involving private-sector entities in marketing and enrollment. Language in the bill would mandate that PreCheck screening lanes be open and available during peak and high-volume travel times.

One concern raised about PreCheck and the passenger screening process is the posting of instructions on publicly accessible Internet sites detailing how to decipher boarding passes to determine whether a passenger is a PreCheck participant, or a Selectee who must undergo thorough secondary screening. The lack of encryption and the limited capability TSA has to authenticate boarding passes and travel documents could be exploited to attempt to avoid detection of threat items by more extensive security measures. To address this concern, the DHS Office of Inspector General recommended in 2015 that TSA explore the feasibility of encrypting boarding passes and work to deploy functional credential authentication technologies at airport screening checkpoints.[94]

Other concerns raised over the PreCheck program include the lack of biometric identity authentication and the extensive use of a program called "managed inclusion" to route selected travelers not enrolled in the PreCheck program through designated PreCheck expedited screening lanes. In 2014, the Government Accountability Office (GAO) found that TSA had not fully tested its managed inclusion practices, and recommended that TSA take steps to ensure and document that testing of the program adheres to established evaluation design practices.[95]

TSA phased out the managed inclusion program in the fall of 2015. Since September 2015, TSA behavior detection officers and explosives trace detection personnel no longer direct passengers

---

[92] See https://www.dhs.gov/trusted-traveler-comparison-chart.

[93] Department of Homeland Security, Transportation Security Administration, Fiscal Year 2016 Congressional Justification, Aviation Security.

[94] Department of Homeland Security, Office of Inspector General, *Use of Risk Assessment within Secure Flight (Redacted)*, OIG-14-153, Washington, DC, July 2015, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_14-153_Jul15.pdf.

[95] U.S. Government Accountability Office, *Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments*, GAO-15-150, December 2014.

not enrolled in PreCheck to expedited screening lanes. Selections based on evaluations by canine explosives detection teams continue, but TSA is moving toward offering expedited screening only to PreCheck program enrollees.[96]

In addition to passenger screening, TSA, in coordination with participating airlines and labor organizations representing airline pilots, has developed a known-crewmember program to expedite security screening of airline flight crews.[97] In July 2012, TSA expanded the program to include flight attendants.[98] The program is currently available at several airports in the United States, but is not available to foreign aircrews or at foreign airports.

Behavioral Detection Approaches

TSA has developed a passenger behavior detection program to identify potential threats based on observed behavioral characteristics. TSA initiated early tests of its Screening Passengers by Observational Techniques program in 2003. By FY2012, the program deployed almost 3,000 Behavior Detection Officers at 176 airports, at an annual cost of about $200 million.

Despite its significant expansion, questions remain regarding the effectiveness of the behavioral detection program, and privacy advocates have cautioned that it could devolve into racial or ethnic profiling of passengers despite concerted efforts to focus solely on behaviors rather than individual passenger traits or characteristics. While some Members of Congress have sought to shutter the program, Congress has not approved legislation to do so. For example, H.Amdt. 127, an amendment to the FY2014 DHS appropriations measure that sought to eliminate funding for the program, failed to pass a floor vote in the 113th Congress. Congress also has not taken specific action to revamp the program, despite concerns raised by GAO and the DHS Office of Inspector General.[99] Congress has, however, repeatedly directed TSA to provide justification for the program and evidence of its utility and effectiveness, mostly through appropriations report language.

Terrorist Watchlists in Aviation

After the failed bombing attempt of Northwest Airlines flight 253 on December 25, 2009, TSA modified security directives to require airlines to check passenger names against the No Fly List within two hours of being electronically notified of an urgent update, instead of allowing 24 hours to recheck the list. The event also accelerated the transfer of watchlist checks from the airlines to TSA under the Secure Flight program, the mechanism for vetting passenger name records against

---

[96] "TSA Explains Confusion over PreCheck Policies," *TravelSkills*, September 23, 2015, http://travelskills.com/2015/09/23/tsa-explains-confusion-over-precheck-policies/.

[97] See http://www.knowncrewmember.org/Pages/Home.aspx.

[98] Transportation Security Administration, *Press Release: U.S. Airline Flight Attendants to Get Expedited Airport Screening in Second Stage of Known Crewmember Program*, July 27, 2012, http://www.tsa.gov/press/releases/2012/07/27/us-airline-flight-attendants-get-expedited-airport-screening-second-stage.

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

the No Fly and Selectee lists. In November 2010, DHS announced that 100% of passengers flying to or from U.S. airports were being vetted using Secure Flight.[100]

On international flights, Secure Flight operates in coordination with the use of watchlists maintained by CBP's National Targeting Center-Passenger, which relies on the Advance Passenger Information System, the ATS-P, and other tools to vet both inbound and outbound passenger manifests.

In addition to these systems, TSA conducts risk-based analysis of passenger data carried out by the airlines through use of the Computer-Assisted Passenger Prescreening System (CAPPS). In January 2015, TSA gave notification that it would start incorporating the results of CAPPS assessments, but not the underlying data used to make such assessments, into Secure Flight along with each passenger's full name, date of birth, and PreCheck traveler number (if applicable). These data were used within the Secure Flight program to perform risk-based analyses to determine whether passengers receive expedited, standard, or enhanced screening at airport checkpoints.[101] Use of Secure Flight to select passengers for expedited screening has been discontinued following concerns that the practice created security vulnerabilities and recommendations that it be discontinued by the DHS Office of Inspector General following an incident in which a convicted domestic terrorist was selected to receive expedited airport screening based on results of the TSA Secure Flight risk-based analysis.[102]

Passenger 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 modified, if warranted, 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 erroneous information corrected.[103]

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.[104] The DHS TRIP program allows passengers seeking redress, or their representatives, to file complaints online or by mail.[105] After receiving the completed online questionnaire or the complaint form, DHS is to request supporting information

---

[100] Department of Homeland Security, "DHS Now Vetting 100 Percent of Passengers On Flights Within Or Bound For U.S. Against Watchlists," press release, November 30, 2010.

[101] Department of Homeland Security, Transportation Security Administration, "Privacy Act of 1974; Department of Homeland Security Transportation Security Administration-DHS/TSA-019 Secure Flight Records System of Records," 80 *Federal Register* 233-239, January 5, 2015.

[102] Department of Homeland Security, Office of Inspector General, *Allegation of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679) (Redacted)*, OIG-15-45, Washington, DC, March 15, 2015, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-45_Mar15.pdf.

[103] See 49 U.S.C. §44926.

[104] See https://www.dhs.gov/dhs-trip.

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

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 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.[106]

DHS has revised the manner in which redress cases are handled after a number of courts determined that the procedures for seeking redress violated individuals' rights to due process under the Constitution.[107] Under the revised redress process now in place, a U.S. person[108] who applies for redress from an allegedly erroneous inclusion on the No Fly List would receive an initial response letter indicating whether he or she is in fact on the No Fly List. If so, this letter would also notify the individual that he or she may elect to receive or submit additional information. These processes generally do not apply to foreign citizens as such individuals have no specific legal rights to redress under current law.

If the individual requests further information, DHS TRIP will forward the details of the case to the TSC Redress Office, which in turn would notify NCTC and the relevant nominating agencies that a redress submittal has included a request for additional information concerning an individual's placement on the No Fly List. The TSC Redress Office would then request an unclassified summary of information supporting an individual's placement on the No Fly List. Upon receipt of this information, the TSC would forward it to DHS TRIP, which would typically provide a second response to the redress seeker that would include details of the unclassified summary provided by the TSC. This second letter informs recipients that they may seek further review of their status and that they may submit any information supporting the position that their placement on the No Fly List is not warranted.

The TSC Redress Office will review the relevant materials provided by federal agencies and the redress seeker and provide a recommendation to the TSA Administrator regarding whether or not the individual should remain on the No Fly List. The TSA Administrator would review that recommendation and issue a final decision to remove the individual from the No Fly List, maintain the individual on the list, or remand the case to TSC for further information. This final order would be sent to the individual petitioner and TSC. If the order removes the individual from the No Fly List, the TSC would update the relevant information in the TSDB.[109]

---

[106] 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.

[107] CRS Report R43730, *Terrorist Databases and the No Fly List: Procedural Due Process and Other Legal Issues*, by (name redacted)

[108] U.S. person refers to a citizen or Lawful Permanent Resident.

[109] For further details on the revised redress procedures, see Declaration of G. Clayton Grigg, Deputy Director for Operations of the Terrorist Screening Center, Latif v. Holder (D. Or. 2015) (No. 3:10-cv-00750-BR 4), available at https://www.aclu.org/sites/default/files/field_document/253%20Declaration%20of%20G%20Clayton%20Grigg_0.pdf.

2

List of Abbreviations

ATS	Automated Targeting System
ATS-P	Automated Targeting System-Passenger
CAPPS	Computer-Assisted Passenger Prescreening System
CBP	Customs and Border Protection
CCD	Consular Consolidated Database
CLASS	Consular Lookout and Support System
DHS	Department of Homeland Security
DHS TRIP	Department of Homeland Security Traveler Redress Inquiry Program
DOS	Department of State
ESTA	Electronic System for Travel Authorization
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
INA	Immigration and Nationality Act
KFE	Kingfisher Expansion
KST	Known or Suspected Terrorist
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
SAO	Security Advisory Opinion
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
VWP	Visa Waiver Program

Author Contact Information

(name redacted)
Specialist in Organized Crime and Terrorism
[redacted]@crs.loc.gov, 7-....

(name redacted)
Specialist in Aviation Policy
[redacted]@crs.loc.gov, 7-...

(name redacted)
Specialist in Immigration Policy
[redacted]@crs.loc.gov, 7-....

Acknowledgments