United States Government Accountability Office

Testimony before the Subcommittee on Transportation Security, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Thursday, September 18, 2014

SECURE FLIGHT

Additional Actions Needed to Determine Program Effectiveness and Strengthen Privacy Oversight Mechanisms

Statement of Jennifer Grover, Acting Director,
Homeland Security and Justice

Chairman Hudson, Ranking Member Richmond, and Members of the Subcommittee:

I am pleased to be here today to discuss the findings from our two September 2014 reports, being released today, in which we assessed the performance of the Department of Homeland Security (DHS) Transportation Security Administration's (TSA) Secure Flight program and related privacy issues.[1] Secure Flight screens approximately 2 million passengers each day, matching passenger information against federal government watchlists and other information to assign each passenger a risk category. By identifying those passengers who may pose security risks, Secure Flight helps protect against potential acts of terrorism that might target the nation's civil aviation system.

In response to requirements of the Intelligence Reform and Terrorism Prevention Act of 2004, and a recommendation of the National Commission on Terrorist Attacks upon the United States (the 9/11 Commission), TSA developed and implemented Secure Flight in order to assume from air carriers the function of matching passengers against watchlists maintained by the federal government.[2] At the time, TSA matched passengers against two watchlists, which were intended to identify high-risk individuals: (1) the No Fly List, composed of individuals who should be precluded from boarding an aircraft, and (2) the Selectee List, composed of individuals who should receive enhanced screening at the airport security checkpoint. The No Fly and Selectee Lists are subsets of the Terrorist Screening Database (TSDB)—the U.S. government's consolidated watchlist of known or suspected terrorists maintained by the Terrorist Screening Center (TSC), a multiagency organization administered by the Federal Bureau of Investigation.

[1]GAO, *Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness,* GAO-14-531 (Washington, D.C.: Sept. 9, 2014), and *Secure Flight: TSA Could Take Additional Steps to Strengthen Privacy Oversight Mechanisms,* GAO-14-647 (Washington, D.C.: Sept. 9, 2014).

[2]See Pub. L. No. 108-458, § 4012(a), 118 Stat. 3638, 3714-18 (2004) (codified at 49 U.S.C. § 44903(j)(2)(C)). The 9/11 Commission, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, July 2004. TSA efforts to develop a computer-assisted passenger prescreening system predated the Intelligence Reform and Terrorism Prevention Act and the report of the 9/11 Commission.

After initiating development of Secure Flight in August 2004, TSA began implementing it in 2009, and completed transitioning foreign and domestic air carriers to the program in November 2010.[3] Secure Flight now screens passengers and certain nontraveling individuals on all domestic and international commercial flights to, from, and within the United States; certain flights overflying the continental United States; and international point-to-point flights operated by U.S. aircraft operators.[4]

Secure Flight can have inadvertent and potentially inappropriate impacts on the traveling public, such as when passengers are identified as high risk because they share a similar name and date of birth with an individual listed on a watchlist, and thus experience delays and inconveniences during their travels. DHS's Traveler Redress Inquiry Program (DHS TRIP) provides passengers who have been denied boarding, or identified for additional screening, with an opportunity to be cleared if they are determined not to be a match to TSDB-based watchlist records (i.e., misidentified) or if they have been wrongly identified as the subject of a TSDB watchlist record (i.e., mislisted).[5]

My testimony today highlights the key findings of our two reports on Secure Flight.[6] My statement will address the extent to which (1) TSA's performance measures appropriately assess progress toward achieving

[3]TSA began implementing Secure Flight pursuant to the Secure Flight Program Final Rule, issued in October 2008. See 73 Fed. Reg. 64,018 (Oct. 28, 2008).

[4]Secure Flight screens certain nontraveling individuals, such as escorts for minor, elderly, and disabled passengers, who are authorized to access the airport's sterile area—the portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which access is generally controlled through the screening of persons and property. See 49 C.F.R. § 1540.5. For purposes of this report, the term "commercial flight" encompasses all U.S. and foreign air carrier operations covered by and subject to the Secure Flight Final Rule. See 49 C.F.R. § 1560.3 (defining "covered flight" for purposes of the Secure Flight Program).

[5]DHS established DHS TRIP in February 2007 as the central processing point within DHS for travel-related redress inquiries. See 49 U.S.C. § 44903(j)(2)(G)(i) (requiring the establishment of a timely and fair process for individuals identified as a threat as a result of TSA's passenger prescreening system to appeal the determination and correct any erroneous information).

[6]GAO-14-531 addressed the operations of the Secure Flight program, including TSA's implementation of screening determinations at the checkpoint and performance measures for the Secure Flight program. GAO-14-647 addressed Secure Flight's privacy oversight mechanisms and DHS's redress process.

the Secure Flight program goals, (2) TSA ensures that Secure Flight screening determinations for passengers are fully implemented at airport security checkpoints, (3) DHS's redress process addresses the delays and inconveniences that result from Secure Flight screening, and (4) TSA has implemented privacy oversight mechanisms to address Secure Flight privacy requirements.

For the September 2014 reports, we analyzed documentation of TSA's program goals and performance measures for fiscal years 2011 through 2013 and assessed these measures against provisions of the Government Performance and Results Act (GPRA).[7] We also analyzed a list that TSA compiled at our request of missed passengers on two high-risk lists (including the reasons for these matching errors) that occurred from November 2010 through July 2013. We analyzed certain TSA data on screener performance at airport security checkpoints from May 2012, when TSA began tracking these data, through February 2014, when we conducted the analysis. We also reviewed relevant DHS TRIP redress and appeals data for fiscal years 2011 through 2013. In addition, to evaluate TSA's documentation of Secure Flight privacy issues and decisions and TSA's privacy training for Secure Flight staff, we reviewed relevant documents prepared by TSA privacy officials and contract staff, including privacy compliance validation reports for the period from April 2012 through April 2013, monthly status reports prepared by TSA's privacy contractor for the period from March 2013 through April 2014, and privacy training documents. We interviewed TSA and other DHS officials who are responsible for aspects of Secure Flight and DHS TRIP, as well as TSA officials at nine airports, which we selected based on a variety of factors, such as volume of passengers screened and geographic dispersion. Our September 2014 reports provide further details on our scope and methodology.[8] The work upon which this statement is based was conducted in accordance with generally accepted government auditing standards.

[7]Government Performance and Results Act of 1993, Pub. L. No. 103-62, 107 Stat. 285 (1993). GPRA was updated by the GPRA Modernization Act of 2010. Pub. L. No. 111-352, 124 Stat. 3866 (2011).

[8]GAO-14-531 and GAO-14-647.

Background

Since its implementation in 2009, Secure Flight has changed from a program that identifies passengers as high risk solely by matching them against the No Fly and Selectee Lists to one that assigns passengers a risk category: high risk, low risk, or unknown risk. In 2010, following the December 2009 attempted attack on a U.S.-bound flight, which exposed gaps in how agencies used watchlists to screen individuals, TSA began using risk-based criteria to identify additional high-risk passengers who may not be in the TSDB, but who should be subject to enhanced screening procedures. Further, in 2011, TSA began screening passengers against additional identities in the TSDB that are not already included on the No Fly or Selectee Lists. In addition, as part of TSA Pre✓™, a 2011 program through which TSA designates passengers as low risk for expedited screening, TSA began screening against several new lists of preapproved low-risk travelers. TSA also began conducting TSA Pre✓™ risk assessments, an activity distinct from matching against lists that uses the Secure Flight system to assign passengers scores based upon their travel-related data, for the purpose of identifying them as low risk for a specific flight. See appendix I for a list of Secure Flight screening activities.

To conduct Secure Flight screening, TSA uses passenger information, known collectively as Secure Flight Passenger Data (SFPD), which is collected by aircraft operators.[9] Once this screening is conducted, Secure Flight then sends the air carrier a determination of how the passenger will be screened at the checkpoint if provided a boarding pass. These determinations include a "TSA Pre✓™ eligible" message for passengers who may receive expedited screening; a "cleared" message for passengers found not to match any high- or low-risk list and who, therefore, will generally receive standard screening; and a "selectee"

[9]See 49 C.F.R. § 1560.3. SFPD includes personally identifiable information, such as full name, gender, date of birth, passport information (if available), and certain nonpersonally identifiable information, such as itinerary information and the unique number associated with a travel record (record number locator).

message for passengers who should undergo enhanced screening.[10] For passengers matching the No Fly List, the air carrier is precluded from issuing a boarding pass.

Passengers who believe they have been unfairly denied boarding or identified for additional screening may apply to DHS TRIP using an online application, by e-mail, or by mail. If DHS TRIP determines that an individual is still a potential match to a TSDB watchlist record, it refers the matter to TSC for further review. TSC then conducts its own review of whether the individual has been misidentified to a watchlist and whether, based on the most current available information and criteria for inclusion on the list, the individual is either correctly assigned to the list or is wrongly assigned and should be removed from the list. If DHS TRIP and TSC determine that no change in the passenger's status is warranted, the passenger is notified of this decision, and depending on the determination, some passengers are permitted the opportunity to appeal the decision. When passengers appeal, DHS TRIP forwards all completed appeals paperwork to TSC. TSC analysts are to review all derogatory information maintained on the appellant to make a written recommendation to TSA on the appeal. TSA then reviews TSC's recommendation through its own internal process, which can include going back to TSC for additional information, before the TSA Administrator makes the final determination to uphold the appellant's status, recommend that TSC downgrade the appellant to another TSDB-based list, or recommend that TSC remove the appellant from the list.[11]

[10]Standard screening typically includes passing through a walk-through metal detector or Advanced Imaging Technology screening, which identifies objects or anomalies on the outside of the body, and X-ray screening for the passenger's accessible property. Enhanced screening includes, in addition to the procedures applied during a typical standard screening experience, a pat-down and an explosive trace detection search or physical search of the interior of the passenger's accessible property, electronics, and footwear. Expedited screening typically includes walk-through metal detector screening and X-ray screening of the passenger's accessible property, but unlike in standard screening, travelers do not have to, among other things, remove their belts, shoes, or light outerwear. The Secure Flight system may also return an error response to air carriers regarding passengers for whom Secure Flight has received incomplete data.

[11]TSC, in the course of its review, may also find the appellant was misidentified to a TSDB-based list.

TSA Lacks Key Information to Determine whether the Secure Flight Program Is Achieving Its Goals

In September 2014, we reported that Secure Flight has established program goals that reflect new program functions since 2009 to identify additional types of high-risk and also low-risk passengers; however, current program performance measures do not allow Secure Flight to fully assess its progress toward achieving all of its goals. For example, to measure performance toward its goals that address the system's ability to accurately identify passengers on various watchlists, Secure Flight collects various types of data, including the number of passengers TSA identifies as matches to high- and low-risk lists. However, we found that Secure Flight does not have measures to assess the extent of system matching errors—for example, the extent to which Secure Flight is missing passengers who are actual matches to these lists. In addition, we found that Secure Flight's measures do not provide information on progress toward the program's goal to incorporate additional risk-based security capabilities to streamline processes and accommodate additional aviation populations, in part because the goal itself did not specify how performance toward the goal should be measured.

We concluded that additional measures that address key performance aspects related to program goals, and that clearly identify the activities necessary to achieve goals, in accordance with the Government Performance and Results Act, would allow TSA to more fully assess progress toward its goals. For example, a measure that reflects misidentifications to all high-risk lists could help TSA appropriately gauge its performance with respect to its goal of limiting such misidentifications. Likewise, establishing measures that clearly represent the performance necessary to achieve the program's goal that addresses risk-based security capabilities will allow Secure Flight to determine the extent to which it is meeting its goal of adapting the Secure Flight system for different risk-based screening activities. Without measures that provide a more complete understanding of Secure Flight's performance, TSA cannot compare actual with desired results to understand how well the system is achieving these goals. Therefore, we recommended in September 2014 that TSA develop additional measures to address key performance aspects related to each program goal, and ensure these measures clearly identify the activities necessary to achieve progress toward the goal. DHS concurred with our recommendation and stated that TSA's Office of Intelligence and Analysis (OIA) will evaluate its current Secure Flight performance goals and measures and develop new performance measures as necessary.

We also found in September 2014 that TSA lacks timely and reliable information on all known cases of Secure Flight system matching errors.

TSA officials told us at the time of our review that when TSA receives information related to matching errors of the Secure Flight system, the Secure Flight Match Review Board reviews this information to determine if any actions could be taken to prevent similar errors from happening again.[12] We identified instances in which the Match Review Board discussed system matching errors, investigated possible actions to address these errors, and implemented changes to strengthen system performance. However, we also found that TSA does not have readily available or complete information on the extent and causes of system matching errors. We recommended that TSA develop a mechanism to systematically document the number and causes of the Secure Flight system's matching errors, in accordance with federal internal control standards. Such a mechanism would provide Secure Flight more timely and reliable information on the extent to which the system is performing as intended. DHS concurred with our recommendation and stated that TSA's OIA will develop a more robust process to track all known cases in which the Secure Flight system has made a matching error, and that the Secure Flight Match Review Board will conduct reviews to identify potential system improvement measures on a quarterly basis.

TSA Has Processes in Place to Implement Secure Flight Screening Determinations at Checkpoints, but Could Take Further Action to Address Screening Errors

In September 2014, we reported that TSA has processes in place to implement Secure Flight screening determinations at airport checkpoints, but could take steps to enhance these processes. Screening personnel at airport checkpoints are primarily responsible for ensuring that passengers receive a level of screening that corresponds to the level of risk determined by Secure Flight by verifying passengers' identities and identifying passengers' screening designations. TSA information from May 2012 through February 2014 that we assessed indicates that screening personnel have made errors in implementing Secure Flight determinations at the checkpoint. TSA officials we spoke with at five of the nine airports where we conducted interviews conduct after-action reviews of screening errors at the checkpoint and have used these reviews to take action to address the root causes of those errors. However, we found that TSA does not have a systematic process for evaluating the root causes of these screening errors at the checkpoint across airports, which could allow TSA to identify trends across airports and target nationwide efforts to address these issues.

[12]Secure Flight's Match Review Board—a multidepartmental entity—and associated Match Review Working Group review performance measurement results and recommend changes to improve system performance, among other things.

Officials with TSA's Office of Security Operations (OSO) told us in the course of our September 2014 review that evaluating the root causes of screening errors would be helpful and stated they were in the early stages of forming a group to discuss these errors. However, TSA was not able to provide documentation of the group's membership, purpose, goals, time frames, or methodology. *Standards for Internal Control in the Federal Government* states that managers should compare actual performance with expected results and analyze significant differences.[13] Therefore, we recommended in September 2014 that TSA develop a process for evaluating the root causes of screening errors at the checkpoint and then implement corrective measures to address those causes. DHS concurred with our recommendation and stated that TSA's OSO will collect and evaluate data on screening errors to identify root causes and work to implement corrective measures. Uncovering and addressing the root causes of screening errors could allow TSA to strengthen security screening at airports by reducing the number of these errors at the checkpoint.

[13]GAO, *Internal Control: Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1. (Washington, D.C.: Nov. 1, 1999).

DHS TRIP Addresses Inconveniences and Delays Related to TSDB-Based Lists, and Is Taking Actions to Reduce Case-Processing Time

In September 2014, we reported that DHS TRIP affords passengers adversely affected by TSA screening processes an opportunity to address inconveniences and delays associated with being potentially misidentified to a TSDB-based list.[14] Passengers who are determined to have been incorrectly matched to or listed on high-risk lists based on the TSDB are added to a list of passengers known as the TSA Cleared List, which allows them to be cleared (not identified as high risk) nearly 100 percent of the time.[15] The DHS TRIP process also allows passengers determined to have been improperly included on a TSDB-based list (mislisted) to be removed, minimizing the likelihood they will be identified as matches during future travels.[16] Although DHS TRIP is not able to provide redress

[14]The specific impacts experienced by a passenger who has been matched to a watchlist vary depending upon the list to which the passenger is matched. For example, an individual with a name similar to that of someone who is on the No Fly list likely will be unable to utilize the convenience of Internet, curbside, and airport kiosk check-in options.

[15]Upon receipt of a complete application, DHS TRIP sends a notification of receipt with a redress control number to the passenger. DHS TRIP adds the name, date of birth, and redress control number of applicants determined not to match a TSDB-based list to the TSA Cleared List. Passengers included on the TSA Cleared List must then submit their redress control number when making a reservation to allow the Secure Flight system to recognize and clear them. Because of the application of other TSA security measures, such as random selection, an individual's presence on the Cleared List may diminish, but will not preclude, the possibility of being selected for enhanced screening.

[16]During the pendency of this review, various courts have issued decisions relating to the No Fly List and DHS TRIP. For example, in January 2014, a judge of the U.S. District Court for the Northern District of California issued a findings of fact, conclusions of law, and order for relief in the case of *Ibrahim v. Dep't of Homeland Security*, No. C 06-00545 WHA (N.D. Cal. Jan 14, 2014) (redacted). Specifically, the court found that in this matter, which involved facts dating back to 2004, the plaintiff had been placed on the No Fly List as a result of a Federal Bureau of Investigation agent's human error and that, among other things, the redress response letter provided to the plaintiff by the redress program in place prior to the establishment of DHS TRIP was inadequate at the time because the response was vague and "fell short of providing any assurance to [the Plaintiff] . . . that the mistake had been traced down in all its forms and venues and corrected." In June 2014, a judge of the U.S. District Court for the District of Oregon issued an opinion and order concluding, among other things, that because DHS TRIP procedures do not afford individuals the requirements of due process in so much as they do not provide them with notice regarding their status on the No Fly List and the reasons for placement on the list, "the absence of any meaningful procedures to afford Plaintiffs the opportunity to contest their placement on the No Fly List violates Plaintiffs' rights to procedural due process." See *Latif v. Holder*, No. 3:10-cv-00750-BR (D. Or. June 24, 2014). According to a Joint Supplemental Status Report filed with the district court on September 3, 2014, the government is in the process of developing revised procedures and is committed to complete this and other steps and issue final orders prior to February 2, 2015. Our review focused on the procedures and data relating to implementation of the DHS TRIP redress and appeals processes and did not evaluate DHS TRIP on sufficiency of procedural due process grounds.

for passengers who may have been misidentified to high-risk, rules-based lists (TSA's lists of high-risk passengers who, based on risk-based criteria, should be subject to enhanced screening procedures though they may not be in the TSDB), according to TSA officials, TSA procedures for using such lists mitigate impacts on these passengers. These procedures may result in TSA removing passengers from the lists, which ensures that passengers who are misidentified to those individuals will no longer be identified as a match, and thus delayed or inconvenienced as a result.

We also found that DHS has reduced its average processing time for redress cases and is taking actions to further reduce processing times. Specifically, we found that DHS TRIP officials took several steps in fiscal year 2013 to reduce the overall processing time and a backlog of redress cases including, for example, automating its response to DHS TRIP applicants and hiring additional staff. According to DHS TRIP officials, at the beginning of fiscal year 2014, DHS TRIP's average case-processing time for redress cases was approximately 100 days, and as of June 2014, the average case-processing time was about 42 days. In January 2014, DHS TRIP also reduced its target for one of its key performance indicators—average number of days for DHS TRIP redress cases to be closed—from 93 to 78 days.

In addition, we reported in September 2014 that DHS TRIP is taking actions to reduce processing times for appeals cases. Appeals applicants receive a letter stating that DHS will provide a final agency decision on the appeal within 60 days of receipt of the appeal. However, we found that the average total processing time for the appeals process for fiscal years 2011 through 2013 was 276 days. In fiscal year 2013, DHS TRIP began taking several actions to make the appeals process more structured and reduce the overall review time, including, among other things, developing and distributing documents that provide information on the status and outcome of each appeal case and implementing a more formalized process for reviewing appeals. In January 2014, DHS TRIP also established intermediate and long-term performance goals for the appeals process for the first time. Specifically, the intermediate performance goal calls for an average total processing time of 92 days, while the long-term performance goal calls for an average processing time of 60 days, consistent with the time frame DHS TRIP commits to achieving in the letter informing applicants of their right to appeal. According to DHS TRIP officials, the agency plans to periodically assess its progress toward achieving its intermediate and long-term goals for reducing appeals-processing times. Officials stated that if DHS TRIP finds it is not making adequate progress by February 2015—about 1 year after

the program began taking specific actions to reduce the overall review time—it would first evaluate whether further changes and improvements could be made to shorten the appeals process before considering, in collaboration with TSC and the DHS Screening Coordination Office, a change to the 60-day time frame stated in the appeals letter.

TSA Has Implemented Oversight Mechanisms to Address Passenger Privacy Requirements, but Additional Actions Could Better Ensure Full Compliance

TSA has taken steps to implement privacy oversight mechanisms, but, as we reported in September 2014, additional actions could allow TSA to sustain and strengthen its efforts. Overall, TSA has implemented mechanisms to identify privacy implications associated with program operations and address them as necessary. For example, TSA has regularly updated privacy documents to address changes in the Secure Flight program and maintains and reviews audit logs of Secure Flight system and user events, such as requests to access the system that generates reports on Secure Flight activities. TSA has also implemented privacy training for new Secure Flight staff, and all DHS employees receive annual privacy training. However, we found that existing Secure Flight staff do not receive job-specific privacy refresher training consistent with Office of Management and Budget (OMB) requirements.[17] For example, TSA updated its privacy training for new Secure Flight staff in December 2013 to reflect new privacy risks unique to Secure Flight's expanded screening activities. However, because the DHS privacy refresher training for existing staff is not job-specific, staff who joined Secure Flight prior to December 2013 may not have received privacy training specific to these new screening activities. We recommended that TSA provide at least annual job-specific privacy refresher training in order to further strengthen Secure Flight's protection of personally identifiable information. DHS concurred with our recommendation and stated that TSA's OIA will develop and deliver job-specific privacy refresher training for all Secure Flight staff.

We also reported in September 2014 that TSA documents some aspects of its Secure Flight privacy oversight mechanisms, such as scheduled destructions of passenger data and reviews of planned changes to the Secure Flight system. However, TSA does not have a mechanism to comprehensively document and track key privacy-related issues and

[17]See Office of Management and Budget, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB Memorandum M-07-16 (Washington, D.C.: 2007).

decisions that arise through the development and use of Secure Flight—a mechanism TSA planned to develop when Secure Flight implementation began in 2009. In the course of our September 2014 review, TSA's Secure Flight privacy officer told us that, in the absence of such a system, Secure Flight relies on its privacy contract staff to oversee and monitor privacy protections, in consultation with the designated Secure Flight program privacy officer and the TSA Privacy Officer. However, it is unknown whether this ad hoc communication would be sustained after a personnel change in Secure Flight's privacy team or contractor personnel, and whether privacy-related decisions previously made would continue to be implemented without documentation to inform new staff. Therefore, to help TSA ensure that these decisions are carried into the future in the event of a change in personnel, we recommended that TSA comprehensively document and track key privacy-related issues and decisions, in accordance with federal internal control standards. DHS concurred with our recommendation and stated that it will develop a mechanism to document such issues and decisions.

Chairman Hudson, Ranking Member Richmond, and members of the subcommittee, this concludes my prepared testimony. I look forward to answering any questions that you may have.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Jennifer Grover at 202-512-7141 or GroverJ@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Maria Strudwick (Assistant Director), Ashley Vaughan (Analyst-in-Charge), Mona Nichols Blake, John De Ferrari, Michele Fejfar, Richard Hung, Tom Lombardi, Erin McLaughlin, and David Plocher.

Appendix I: Secure Flight Screening Activities

Screening activity	Description
No Fly List (high risk)	The No Fly List is a subset of the Terrorist Screening Database (TSDB), the U.S. government's consolidated watchlist of known or suspected terrorists maintained by the Terrorist Screening Center (TSC), a multi-agency organization administered by the Federal Bureau of Investigation. The No Fly List contains records of individuals who are suspected of posing or known to pose a threat to aviation or national security and are prohibited from boarding an aircraft or entering the sterile area of an airport. Secure Flight has matched passengers against the No Fly List since 2009.
Selectee List (high risk)	The Selectee List is a subset of the TSDB containing records of individuals who must undergo enhanced security screening before being permitted to enter the sterile area or board an aircraft. Secure Flight has matched against the Selectee List since 2009.
Expanded Selectee List (high risk)	The Expanded Selectee List includes terrorist records in the TSDB with a complete name and date of birth that meet the reasonable suspicion standard to be considered a known or suspected terrorist, but that do not meet the criteria to be placed on the No Fly or Selectee Lists.[a] Secure Flight began matching against the Expanded Selectee List in April 2011.
Transportation Security Administration (TSA) rules-based lists (high risk)	The high-risk rules-based lists include two lists of passengers who may not be known or suspected terrorists, but who, according to intelligence-driven, scenario-based rules developed by TSA in consultation with U.S. Customs and Border Protection (CBP), may pose an increased risk to transportation or national security.
Centers for Disease Control and Prevention (CDC) Do Not Board List (high risk)	The CDC Do Not Board List is managed by CDC. It includes individuals who pose a significant health risk to other travelers and are not allowed to fly.
TSA Pre✓™ lists (low risk)	TSA Pre✓™ lists include lists of preapproved, low-risk travelers, such as certain members of CBP's Trusted Traveler programs, members of the U.S. armed forces, Congressional Medal of Honor Society members, and Members of Congress—groups of individuals TSA has determined pose a low risk to transportation or national security—as well as a TSA Pre✓™ list created by TSA and composed of individuals who apply and are preapproved as low-risk travelers through the TSA Pre✓™ Application Program.[b] Secure Flight began matching against its first set of low-risk lists, CBP Trusted Traveler Lists, in October 2011 and instituted the TSA Pre✓™ Application Program in December 2013.
TSA Pre✓™ Disqualification List (ineligible for low risk)	The TSA Pre✓™ Disqualification List is a list of individuals who, based upon their involvement in violations of security regulations of sufficient severity or frequency (e.g., bringing a loaded firearm to the checkpoint), are disqualified from receiving expedited screening for some period of time or permanently.
TSA Pre✓™ risk assessments (low risk)	Secure Flight assesses certain travel-related information submitted by passengers and assigns them scores that correspond to a likelihood of being eligible for expedited screening for a specific flight. Secure Flight began performing these assessments for selected frequent flier members in October 2011 and, in October 2013, began using them to evaluate all passengers not determined to be a match to a high-risk or low-risk list.

Source: GAO analysis of TSA and TSC information. | GAO-14-796T

[a]All TSDB-based watchlists utilized by the Secure Flight program contain records determined to have met TSC's reasonable suspicion standard. In general, to meet the reasonable suspicion standard, the agency nominating an individual for inclusion in the TSDB must consider the totality of information available that, taken together with rational inferences from that information, reasonably warrants a determination that an individual is known or suspected to be or have been knowingly engaged in conduct constituting, in preparation for, in aid of, or related to terrorism or terrorist activities. To be included on the No Fly and Selectee Lists, individuals must meet criteria specific to these lists. The TSDB, which is the U.S. government's consolidated watchlist of known or suspected terrorists, also contains records on additional populations of individuals that do not meet the reasonable suspicion

standard articulated above but that other federal agencies utilize to support their border and immigration screening missions. In addition, according to TSA officials, Secure Flight does not utilize all terrorist records in the TSDB because records with partial data (i.e., without first name, surname, and date of birth) could result in a significant increase in the number of passengers misidentified.

[b]Individuals on all low-risk lists receive a Known Traveler Number that they must submit when making travel reservations to be identified as low risk. See 49 C.F.R. § 1560.3 (defining "Known Traveler Number"). TSA also refers to these lists as Known Traveler lists.