Privacy Impact Assessment Update
for

Secure Flight

Silent Partner and Quiet Skies

DHS/TSA/PIA-018(i)

April 19, 2019

Contact Point
Thomas Bush
Intelligence and Analysis
Transportation Security Administration
TSA.OIA.execsec@tsa.dhs.gov

Reviewing Official
Jonathan R. Cantor
Chief Privacy Officer (Acting)
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) leverages its access to the United States Customs and Border Protection (CBP) Automated Targeting System (ATS) to identify individuals for enhanced screening during air travel through use of rules based on current intelligence as part of its Secure Flight vetting process. This PIA describes two specific TSA uses of that capability.

1. TSA's Silent Partner program enables TSA to identify passengers for enhanced screening on international flights bound for the United States.
2. Under TSA's Quiet Skies program, TSA uses a subset of the Silent Partner rules to identify passengers for enhanced screening on some subsequent domestic and outbound international flights.

The Silent Partner and Quiet Skies programs add another layer of risk-based security by identifying individuals who may pose an elevated security risk in addition to individuals on other watch lists maintained by the Federal Government, so that TSA can take appropriate actions to address and mitigate that risk. This Privacy Impact Assessment (PIA) update is being conducted to reflect operational and administrative changes to the TSA Secure Flight Program.

Overview

Pursuant to 49 U.S.C. § 114, TSA is responsible for security in all transportation modes. TSA incorporates a variety of different layers of security measures to identify and prevent threats to aviation security, as well as to other transportation modes.

TSA's Secure Flight program:

- Performs watch list matching on carrier-provided traveler information to the No Fly and Selectee portions of the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC), as well as other watch lists to identify individuals who may need additional screening or are prevented from travel.[1]
- Uses Known Traveler information to identify trusted travelers for whom expedited screening at TSA Pre✓® lanes may be appropriate.[2]
- Uses rules based on risk to determine the level of screening for passengers. These rules are based on risk factors presented by a given flight and passenger, the level of screening for a passenger that may change from flight to flight including

[1] *See* Secure Flight PIA August 9, 2007, and all subsequent updates https://www.dhs.gov/publication/dhstsapia-018-tsa-secure-flight
[2] *See* Secure Flight PIA update August 15, 2011

designating low risk travelers for expedited screening, or designating travelers for enhanced screening who may pose an elevated risk.[3]

A number of other layers of security exist, including the use of technology to identify threat items and protocols to select individuals at random for enhanced screening.

CBP ATS is an enforcement and decision support tool used to incorporate risk-based targeting in CBP missions in traveler, cargo, and conveyance security.[4] It is used to identify and prevent terrorists and terrorist weapons from entering the United States, and to identify other violations of United States laws that are enforced by CBP. ATS consists of multiple modules, including a passenger module that focuses on international travel by air, ship, and rail. ATS maintains data provided to airlines and travel agents by or on behalf of air passengers (Passenger Name Records (PNR)) collected by CBP as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001.[5] ATS compares PNR and information within a variety of databases against lookouts and patterns of suspicious activity identified through past investigations and intelligence to assess whether a passenger should receive additional inspection by CBP officers prior to entering or departing the United States.

TSA leverages its access to ATS to add another layer of aviation security by seeking to identify individuals who may pose an elevated security risk prior to international flights. Under Silent Partner, TSA creates rules based on current intelligence for use by ATS to identify passengers for enhanced screening on their international flights bound for the United States. This PIA update discusses two specific rules-based programs.

1. Silent Partner rules are based on a specific potential threat to aviation security or the United States, as assessed by TSA, with respect to international travel to the United States. Once identified by the rule, those passengers are placed on a Silent Partner List that is retained for the period of the international in-bound flight.

2. Quiet Skies rules are a subset of the Silent Partner rules that are aligned to potential aviation security threats within the United States. TSA uses Quiet Skies rules to create a temporary Quiet Skies List to designate passengers who fall within the Quiet Skies subset of rules for enhanced screening on some subsequent domestic and outbound international travel. Individuals will remain on the Quiet Skies List for a period of time.

The Silent Partner List and Quiet Skies List change daily as individuals are added and deleted.

Records reflecting that an individual was selected under Silent Partner will be retained within CBP's ATS for seven years in accordance with CBP's retention schedule, then for an additional eight years in dormant status under which user access is more limited. Records reflecting

[3] *See* Secure Flight PIA update August 15, 2011
[4] *See* DHS/CBP/PIA-006 Automated Targeting System (ATS), *available at* https://www.dhs.gov/privacy.
[5] Pub. L. 107-71, 115 Stat. 597.

that an individual was selected for enhanced screening as a match to the Silent Partner List or Quiet Skies List will be held in TSA's Secure Flight system for seven years in accordance with the Secure Flight records retention schedule. When a passenger selected for enhanced screening as a match to the Silent Partner List or Quiet Skies List is involved in an incident (for example, a prohibited item is found), records will be retained pursuant to normal incident reporting protocols pursuant to DHS/TSA-001 Transportation Security Enforcement Records System SORN.[6]

TSA formulates rules for Silent Partner and Quiet Skies to address unknown and partially identified threats. The risk-based, intelligence-driven rules are not used to deny boarding, but result in a limited number of individuals being identified for enhanced screening and may result in other operational response including observation by the TSA Federal Air Marshal Service (FAMS) while the individual is onboard the flight or in the airport. Individuals matching to Silent Partner and Quiet Skies rules are not considered "known or suspected terrorists" and are not nominated to the Terrorist Screening Database (TSDB) under Homeland Security Presidential Directive 6 merely for falling within a security rule. They may be nominated to the TSDB, however, if they are involved in a security incident that would support such nomination.

The rules are based on aggregated travel data, intelligence, and trend analysis of the intelligence and suspicious activity. Travelers may match a Silent Partner or Quiet Skies rule based upon travel patterns matching intelligence regarding terrorist travel; upon submitting passenger information matching the information used by a partially-identified terrorist; or upon submitting passenger information matching the information used by a Known or Suspected Terrorist.

Since the program was initiated in 2010, TSA's risk-based, intelligence-driven rules are subject to ongoing routine civil rights, civil liberties, privacy, and legal reviews. These reviews focus on whether each rule: (1) is based on current intelligence; (2) identifies a specific potential threat to aviation security or the United States;[7] (3) is deactivated when no longer necessary to address the threat; and (4) is appropriately tailored to minimize the impact on travelers' civil rights, civil liberties, and privacy, and is in compliance with relevant legal authorities, regulations, and DHS policies.

TSA has also created Silent Partner and Quiet Skies Cleared Lists, which are intended to minimize impacts on passengers, to ensure an individual will not indefinitely receive enhanced screening on account of TSA's risk-based, intelligence-driven rules, and to enhance privacy, civil rights, and civil liberties protection in the Quiet Skies program. Passengers who match the Silent Partner List are placed on the Silent Partner Cleared List after a period of time. Passengers who match the Quiet Skies List are placed on the Quiet Skies Cleared List after receiving enhanced screening for a period of time. The exclusion is implemented through an automated process within

[6] *See* DHS/TSA-001 Transportation Security Enforcement Record System, 83 FR 43888 (August 28, 2018).
[7] Silent Partner rules must pertain to a specific potential threat to aviation security or the Homeland, as assessed by TSA; Quiet Skies rules must pertain to a specific potential threat to aviation security within the Homeland, as assessed by TSA.

the Secure Flight program. TSA may add individuals to the Silent Partner Cleared List and Quiet Skies Cleared List on its own initiative when appropriate, including, as a result of filing an application with the Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP).[8]

In order to provide operational awareness prior to scheduling Federal Air Marshal missions, TSA compares the Quiet Skies List against its incident reporting databases (e.g., Web-Based Emergency Operations Center,[9] Performance and Results Information System,[10] Tactical Information Sharing System[11]) and CBP TECS to determine if there may have been previous encounters with the individual that resulted in security incidents or suspicious activity. Prior incidents with the individual might inform TSA's operational response, and may be used for statistical and analytical purposes. TSA may also perform open source research on the Quiet Skies List to inform its operational response or may result in placing the individual on a Cleared List. For example, a simple open web search of the individual may reveal that TSA should place the individual on a Cleared List to avoid diverting security resources and unnecessarily inconveniencing the passenger. Federal Air Marshals prepare after action reports on mission coverage of individuals identified by Silent Partner and Quiet Skies. These reports may document instances in which individuals designated through Quiet Skies were involved in security incidents or suspicious activity; conversely, they may provide information that may be used to place the individual on the Silent Partner and Quiet Skies Cleared Lists.

Individuals on the Silent Partner and Quiet Skies Cleared Lists will remain on these lists for a period of time. During this time period, a passenger would not be referred for enhanced screening due to matching against the same Quiet Skies rule, or against the same or similarly-written Silent Partner rule,[12] but may be referred if they match to a different Quiet Skies rule or a different Silent Partner rule. This period of time is consistent across all Silent Partner and Quiet Skies rules, but is subject to change based upon TSA's assessment of intelligence regarding threats to aviation security posed by individuals who match Silent Partner or Quiet Skies rules, including the impact upon travelers resulting from any reduction in the amount of time for which an individual remains on a Silent Partner or Quiet Skies Cleared List. After a passenger reaches the designated period for exclusion from Silent Partner or Quiet Skies rules, passengers who hit an active Silent Partner or Quiet Skies rule will again be placed on the Silent Partner List and/or Quiet Skies List, and become eligible for the Quiet Skies and Silent Partner Cleared Lists again as described above.

---

[8] *See* DHS/ALL/PIA-002 Department of Homeland Security Traveler Redress Inquiry Program, *available at* www.dhs.gov/privacy.
[9] *See* DHS/TSA/PIA-029 TSA Operations Center Incident Management System, *available at* www.dhs.gov/privacy.
[10] *See* DHS/TSA/PIA-038 Performance and Results Information System, *available at* www.dhs.gov/privacy.
[11] *See* DHS/TSA/PIA-015 Tactical Information Sharing System, *available at* www.dhs.gov/privacy.
[12] For the purposes of operating the Silent Partner Cleared List, the TSA Office of Intelligence &Analysis maintains groups of Silent Partner rules with overlapping or similar data elements that are intended to address the same threat.

Reason for the PIA Update

This Privacy Impact Assessment (PIA) update is being conducted to reflect operational changes and address the programs within a single PIA.

Privacy Impact Analysis

Authorities and Other Requirements

TSA's general operating authorities are set forth in the Aviation and Transportation Security Act (ATSA), 49 U.S.C. § 114(d)-(f). In addition, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[13] specifically directs TSA to test and implement a pre-flight passenger prescreening program, such as Secure Flight. Section 4012(a)(1) of the IRTPA (codified at 49 U.S.C. § 44903(j)(2)) requires TSA to assume from air carriers the comparison of passenger information for domestic flights to the consolidated and integrated terrorist watch list maintained by the Federal Government. Section 4012(a)(2) of IRTPA (codified at 49 U.S.C. § 44909(c)) similarly requires the Department of Homeland Security (DHS) to compare passenger information for international flights to and from the United States against the consolidated and integrated terrorist watch list before departure of such flights.

Pursuant to 49 U.S.C. § 114(f)(2), TSA is required to assess threats to transportation. In addition to screening against the No Fly and Selectee watch lists, when warranted by security considerations, TSA may screen against the full TSDB or other records. TSA has authority under 49 U.S.C. § 114(f) to receive, assess, and distribute intelligence information related to transportation security; to assess threats to transportation; to develop polices, strategies, and plans for dealing with threats to transportation security; and to carry out such other duties and exercise such other powers relating to transportation security as the Administrator considers appropriate. The development of these rules-based programs and integration with Secure Flight were established by TSA to address specific changes observed in how potential terrorists moved from initial radicalization and recruitment to operational readiness. Additionally, pursuant to recommendations by the Government Accountability Office (GAO)[14] and also reflected recently in Section 1959 of the FAA Reauthorization Act of 2018,[15] (amending 49 U.S.C. § 44917(a)), FAMS are required to use a risk-based strategy when allocating resources for international and domestic flight coverage. Incorporating Silent Partner and Quiet Skies into the FAMS deployment strategy enables TSA to meet the risk-based approach required by Congress and further mitigate potential risk across encounters with the same individual during his or her travel lifecycle.

Data from these programs may be stored within systems covered by the following Systems of Records Notices: DHS/TSA-001 Transportation Security Enforcement System (TSERS);

[13] Pub. L. 108-458, 118 Stat. 3638.
[14] GAO-16-582 available at https://www.gao.gov/products/GAO-16-582
[15] Pub. L. 115-254, 131 Stat. 3186.

DHS/TSA-011 Transportation Security Intelligence Service Files (TSIS);[16] and DHS/TSA-019 Secure Flight Records System.[17]

CBP operates ATS under a variety of authorities that cover its several modules, including the required collection of Advance Passenger Information System (APIS)[18] and PNR data pursuant to 49 U.S.C. § 44909. The Automated Targeting System identifies passenger information matching TSA-generated rules, and transmits rule matches to Secure Flight for placement on the SPL or QSL. The DHS/CBP-006 Automated Targeting System SORN[19] and the DHS/CBP/PIA-006 Automated Targeting System describe the system in more detail. The ATS SORN does not change TSA's use of the information maintained in Secure Flight or Transportation Security Intelligence Service SORNs.

HSPD-6

Individuals matching to Silent Partner and Quiet Skies rules are not considered "known or suspected terrorists" or watchlisted under Homeland Security Presidential Directive 6 (HSPD-6), Integration and Use of Screening Information, or the Memorandum of Understanding on the Integration and Use of Screening Information to Protect Against Terrorism (TSC MOU), which founded the TSC and established the consolidated terrorism watch list system. Under HSPD-6 and the TSC MOU, federal agencies are required to provide "terrorist information" in their possession to the National Counterterrorism Center for integration into a terrorism identities database when there is sufficient derogatory information known about the individual to meet the nomination criteria. Specifically, "terrorist information" is defined as "information about individuals known or reasonably suspected to be or to have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism or terrorist activities."

Under the rules-based Silent Partner and Quiet Skies programs, travelers may match a rule based upon travel patterns, intelligence regarding terrorist travel, and/or passenger information correlating with the information used by a partially-identified terrorist or a known or suspected terrorist. Matching a TSA targeting rule is an indication that there may be elevated risk that merits selectee screening. It is not specific derogatory information that the individual has or is suspected to have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism or terrorist activities. If, at a later time, sufficient information beyond the match to a Quiet Skies or Silent Partner rule is obtained such that an individual meets the requirements to be determined to be a known or suspected terrorist, information about that individual will be provided to the TSC, through the processes established under the TSC MOU.[20]

---

[16] *See* DHS/TSA-011 Transportation Security Intelligence Service Files (TSIS), 75 FR 18867, (April 13, 2010).
[17] *See* DHS/TSA-019 Secure Flight Records System, 80 FR 233, (January 5, 2015).
[18] *See* DHS/CBP/PIA-001 Advance Passenger Information System (APIS), *available at* www.dhs.gov/privacy
[19] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297, (May 22, 2012).
[20] *See* Homeland Security Presidential Directive/HSPD-6.

Characterization of the Information

ATS collects and retains information about passengers entering or departing the United States in accordance with United States legal requirements on individuals who make reservations for airline travel. This data includes passenger manifests (through APIS, which also includes crew data for flights overflying the United States), immigration control information, and PNR data. The PNR data may include such items as name, address, email address, phone number, flight, seat number, and other information collected by the airline in connection with a particular reservation. Not all air carriers capture the same amount of information; the number of items captured may even vary among individual PNRs from the same carrier. Information that may be passed by ATS to TSA includes: Automated Targeting System Passenger ID; full name; date of birth; country passport was issued; Passport number; country of birth; departure date; departure airport; arrival airport; airline code; and Rules ID identifying the rule that was triggered. When an individual matches one or more Silent Partner or Quiet Skies rules, ATS transmits the passenger's Secure Flight Passenger Data and an identifier for the particular rule or rules matched to Secure Flight for placement on the Silent Partner List or Quiet Skies List, as appropriate. In addition, as authorized ATS users, TSA can access additional information about an individual that may be contained within ATS including the data elements leading to the rule match, as well as phone numbers, credit card information, reservation agent information, prior encounter information, and other information within ATS.

Secure Flight collects and retains full name, date of birth, gender, redress number (if available), known traveler number (if implemented and available), and passport information (if available) for domestic flights and international flights arriving in, departing from, or overflying the continental United States (defined as the 48 lower contiguous states), as well as international flights operated by U.S. carriers. Secure Flight will maintain the Silent Partner List and Quiet Skies List, as well as a record of individuals who matched to the Silent Partner List and Quiet Skies List during their travel. The TSA Office of Intelligence and Analysis (I&A) will maintain the matches and will correlate these matches with information about incidents to determine whether any Quiet Skies matches also have an incident at the passenger screening checkpoint, within the airport, or during the flight.

TSA rules for ATS are developed by TSA I&A based on current threat information and reviewed on a periodic basis by the DHS Office for Civil Rights and Civil Liberties, the DHS Privacy Office, and the DHS Office of the General Counsel. Prior to activating a rule, TSA tests the rules in CBP ATS to ensure the impact on travelers is no greater than necessary to address the threat identified in current intelligence. These rule sets are applied to international travelers by ATS and generate matches for enhanced screening during their international travel. Individuals matching to Quiet Skies rules will be placed on a Quiet Skies List for enhanced screening on subsequent flights. Not later than 48 hours after changing, updating, implementing, or suspending a Quiet Skies rule, TSA notifies the above listed DHS offices.

The information used by the system is initially provided by the individual passengers to airlines (or to reservations agents). Information transmitted to TSA by the aircraft operators is assumed to be accurate. Identification is required at security checkpoints that will be matched against the boarding pass issued to the passenger by the airline as a further check on accuracy.

Privacy Risk: Because Silent Partner and Quiet Skies matches are not based on specific derogatory information about an individual, individuals who hit against a rule for enhanced screening may be subjected to enhanced screening more often than if TSA only conducted watch list matching based on watch lists of individuals with individualized derogatory information (for example, known or suspected terrorists).

Mitigation: The Silent Partner and Quiet Skies rules are specific intelligence-based rules designed to designate individuals for enhanced screening who may present an elevated security risk but are not on other government watch lists. TSA has developed several mechanisms under which passengers may no longer be required to undergo enhanced screening. These mechanisms include removal from the list at specified time intervals, removal from the list upon deactivation of the applicable rule, removal from the list based on a set number of screenings, DHS TRIP, and the Silent Partner and Quiet Skies Cleared Lists. TSA may also deliberately exclude passengers it determines, in its sole discretion, pose a low risk. The rule sets are routinely reviewed by the DHS Offices for Civil Rights and Civil Liberties, Privacy, and General Counsel.

Privacy Risk: When Secure Flight creates the Quiet Skies List, Secure Flight receives the individual's passport information from ATS. When the airline transmits the Secure Flight Passenger Data (SFPD) for subsequent domestic travel for which a passenger on the Quiet Skies List should receive enhanced screening, it only provides the passport information if it is available. Potentially, a person not on the Quiet Skies List may be incorrectly identified as a match to a person on the Quiet Skies List. There is a risk that passengers with similar names, gender, and date of birth may be selected for enhanced screening for domestic flights even though he or she is not the specific individual that was a match to TSA rule sets within ATS.

Mitigation: Secure Flight applies an algorithm that addresses variations in name spellings and dates of birth. For Quiet Skies, TSA will limit the circumstances under which an individual could be misidentified as a match to the Quiet Skies List by using a match threshold for purposes of determining whether a match exists in the Quiet Skies List for a passenger on a domestic flight, as well as routinely removing names from the Quiet Skies List after the requisite number of encounters or period of time. This should improve accuracy and reduce the potential for misidentification.

Uses of the Information

Silent Partner and Quiet Skies are part of a risk-based security approach to identifying and addressing threats from individuals who potentially pose an elevated risk to aviation security but who may not be in other federal watch lists. Under Silent Partner, TSA creates rules based on

current intelligence for use by ATS to identify passengers for enhanced screening on their international flights bound for the United States. Under Quiet Skies, TSA may identify a subset of the Silent Partner rules that are aligned to potential aviation security threats within the United States to create a temporary Quiet Skies List to designate passengers who fall within the Quiet Skies subset of rules for enhanced screening on some subsequent domestic and outbound international travel. TSA does not use Silent Partner nor Quiet Skies to prohibit boarding. To assist with ensuring that appropriate screening takes place, lists of individuals designated for enhanced screening will be provided to TSA Airport Coordination Centers to ensure that operational staff are aware that the individual should be expected at the airport and ensure appropriate screening. Information from the Silent Partner and Quiet Skies programs will be used by the FAMS as part of the risk analysis conducted to prioritize mission scheduling and may result in observation of the individual at the airport or onboard aircraft. Federal Air Marshal after action reporting will be stored within the TSA Operations Center Incident Management System (OCIMS) system.[21]

Silent Partner results in additional scrutiny necessary to mitigate unknown threats for international flights bound for the United States that triggered a Silent Partner rule. Quiet Skies results in a list of individuals selected for additional scrutiny on subsequent domestic and outbound international flights. Silent Partner and Quiet Skies may be used to designate passengers for enhanced screening, for scheduling of FAMS missions to mitigate the elevated risk, for analytical purposes within TSA I&A, and for oversight, redress, and litigation purposes. If a passenger selected for enhanced screening is involved in an incident at the checkpoint, then normal reporting protocols apply and information about the incident and individual may be shared with law enforcement or others pursuant to the Privacy Act and applicable SORNs (DHS/TSA-001 Transportation Security Enforcement Record System and DHS/TSA-011 Transportation Security Intelligence System).

Privacy Risk: There is a risk that there will be improper disclosure to unauthorized individuals or individuals without a need-to-know.

Mitigation: Authorized users within Secure Flight and TSA I&A, and the DHS TRIP program office for purposes of providing redress, are provided access to systems and data. Name and itinerary are provided to TSA Security Operations and the FAMS for operational purposes. Silent Partner rules are necessarily shared with CBP when running security rules within CBP ATS to generate the international passenger match and for operational reasons involving international passengers who overfly the United States. Both Silent Partner and Quiet Skies information may be shared within DHS or the Department of Justice for redress, litigation, or oversight purposes. Names of individuals on the Silent Partner List and Quiet Skies List are protected as Sensitive Security Information (SSI) and are marked accordingly (including a limitation on disclosure only

[21] *See* DHS/TSA/PIA-029 TSA Operations Center Incident Management System, *available at* www.dhs.gov/privacy.

to those persons with a need to know). TSA issues boarding pass instructions to air carriers that ensure watch list matches receive enhanced screening but does not disclose the status of the passenger to the air carrier. DHS requires that all employees and contractors take annual privacy and information security training. Improper access or disclosure may lead to disciplinary action, including termination.

Privacy Risk: There is a risk that the Silent Partner List or Quiet Skies List may expand beyond the intended purpose of mitigating risk to transportation security.

Mitigation: This risk is mitigated by the specific requirement that uses of the Silent Partner List or Quiet Silent List must mitigate risks to transportation security and that the proposed modifications are subject to periodic review by TSA and DHS offices, including the Office of the General Counsel, Office for Civil Rights and Civil Liberties, and the Privacy Office.

Notice

TSA's use of ATS is generally reflected in the CBP PIA for ATS and in TSA PIAs for Secure Flight. In addition, prior to collecting information from an individual through a website or an airport kiosk with the capability of accepting a reservation, covered aircraft operators are required to make available the following privacy notice, or substantial equivalent approved by TSA, prior to collecting information:

> The Transportation Security Administration is required to collect information from individuals for purposes of watch list matching, under the authority of 49 U.S.C. § 114, and the Intelligence Reform and Terrorism Prevention Act of 2004. Providing this information is voluntary; however, if it is not provided, individuals may be subject to additional screening or denied transport or authorization to enter a sterile area. TSA may share information that is provided with law enforcement or intelligence agencies or others under its published system of records notice. For more on TSA Privacy policies or to view the system of records notice and the privacy impact assessment, please see TSA's web site at www.tsa.gov.

Privacy Risk: There is a risk that individuals do not receive specific notice of Silent Partner or Quiet Skies.

Mitigation: Individuals making flight reservations are provided notice that information will be provided to TSA for use by Secure Flight to conduct watch list checks. This PIA, and other Secure Flight PIAs, provide notice that watch lists can be derived from, among other things, real-time threat-based intelligence scenarios created by TSA and run by CBP's ATS system to identify international travelers requiring enhanced screening, and are therefore on notice that the Federal Government will perform checks on various databases in order to evaluate whether the individual may pose a threat to aviation security.

Data Retention by the project

Silent Partner

Silent Partner data is retained within CBP ATS for seven years in active storage and an additional eight years in a dormant status under which access to the data is more limited (N1-568-074). Authorized TSA users of ATS can access the records in active storage but must request access to dormant records from a senior official and only in response to an identifiable case, threat, or risk. Silent Partner records will also be retained within TSA I&A for seven years for use within its Secure Flight program and for oversight and analysis, redress, and litigation. Federal Air Marshal after action reports will be maintained for five years in accordance with an existing National Archives and Records Administration (NARA) approved records schedule (N1-560-06-5, item 3), but TSA expects to seek approval to reduce the records retention to 90 days for reports indicating no suspicious activity.

Quiet Skies

There are two categories of records generated by Quiet Skies: a watch list of individuals matching TSA rule sets within ATS, and the matches by Secure Flight to the watch list on subsequent flights. Records reflecting the composition of the Quiet Skies List will be updated through addition and deletion within the Secure Flight system as the list is updated (N1-560-08-3, item 1a). Match records (records reflecting that an individual was selected for enhanced screening as a match to the Quiet Skies List) will be held in the Secure Flight system for seven years in accordance with the Secure Flight records retention schedule (N1-560-08-3, item 1e) principally for purposes of oversight, redress, and litigation.

In addition, TSA I&A will retain Quiet Skies records for seven years for oversight and analysis, redress, and litigation and to conform with the record retention for the Secure Flight system. As explained previously, Federal Air Marshal after action reports will be maintained for five years in accordance with an existing NARA approved records schedule (N1-560-06-5, item 3), but TSA expects to seek approval to reduce the records retention to 90 days for these after action reports when no suspicious activity is observed.

When an individual selected for enhanced screening as a match to Quiet Skies is involved in an incident (for example, a prohibited item is found), records will be retained by TSA for three years pursuant to normal incident reporting protocols (N1-560-12-002, item 9).

Privacy Risk: There is a risk that data will be retained for an excessive amount of time.

Mitigation: Retention of data is consistent with existing NARA-approved retention schedules. In addition, TSA expects to seek approval to modify the retention schedules associated with Silent Partner and Quiet Skies records, including by reducing the amount of time for which FAMS retains after action reports of missions for which there was no suspicious activity scheduled on account of Silent Partner or Quiet Skies and is considering increasing the amount of time TSA

I&A retains Silent Partner and Quiet Skies data to seven years, consistent with the record retention schedules for Secure Flight and for active storage within ATS.

Information Sharing

Information about passengers who are selected for enhanced screening under Silent Partner is not shared with parties external to DHS, except for redress, litigation, or oversight purposes in accordance with the Privacy Act and applicable SORN. Information about individuals on the Quiet Skies List, or matched to the list, will not be shared with parties external to DHS, except to the extent the individual may also be on the TSDB or other watch list; is involved in an incident for which external sharing is part of normal incident protocols, such as where suspicious behavior rises to the level of a report under the DHS Nationwide Suspicious Activity Reporting Initiative (DHS NSI) functional standard; or for redress, litigation, or oversight purposes.

Privacy Risk: There is a risk that information may be shared with parties external to DHS for purposes beyond aviation security.

Mitigation: The risk is mitigated by administrative policies to prevent such external sharing, except to the extent the individual may also be on the TSDB or other watch list; is involved in an incident for which external sharing is part of normal incident protocols such as where suspicious behavior rises to the level of a report under the DHS NSI functional standard; or for redress, litigation, or oversight purposes.

Redress

Redress and access information is available to the public through the existing privacy compliance documentation for Secure Flight. Selection for enhanced screening under Silent Partner and Quiet Skies is based on international travel that is confirmed by CBP at the time of re-entry into the United States. Individuals may seek redress through DHS TRIP when they believe they have experienced travel screening-related difficulties such as being unfairly or incorrectly delayed, denied boarding, or identified for additional screening at an airport.

Individuals will not be provided with the basis for their selection for enhanced screening. Because the Silent Partner and Quiet Skies rules are based on current and prior travel, the information leading to a passenger's placement on the Silent Partner List or Quiet Skies List is very likely to be accurate. However, DHS TRIP offers redress for passengers who have been designated for enhanced screening through Silent Partner and Quiet Skies. The redress process includes referral to TSA I&A for consideration for placement on the appropriate cleared list. Additionally, other redress mechanisms have been developed to include deliberate exclusion based on TSA reviews, automated removal from the list at time intervals, automated removal from the Quiet Skies List upon deactivation of the applicable rule, automated removal from the Quiet Skies List based upon a set number of screenings, and the automated use of the Silent Partner Cleared List, the Quiet Skies Cleared List.

Individuals can also seek access to their records by submitting a request under the Privacy Act to:

Transportation Security Administration
Freedom of Information Act Office, TSA-20
601 South 12th Street
Arlington, VA 20598-6020

Requests may also be submitted by email at FOIA.TSA@dhs.gov. The request must contain the following information: full name, address and telephone number, email address (optional), a specific description of the records sought, and a statement regarding your willingness to pay fees.

Privacy Risk: There is a risk that individuals will be selected for repeated additional screening based on factors that cannot be corrected.

Mitigation: TSA mitigates risk through DHS TRIP, use of the Silent Partner and Quiet Skies Cleared Lists, deliberate exclusion on its own initiative, removal from the Quiet Skies List at intervals, removal from the Quiet Skies List based upon a set number of screenings, and removal from the Quiet Skies List upon deactivation of the applicable rule.

Privacy Risk: There is a risk that individuals will be selected for enhanced screening based on erroneous information.

Mitigation: Without passport information to confirm against the identity of the individual who was the match to the TSA rule set within ATS, under very limited circumstances when a traveler has the same name and date of birth as a person on the Quiet Skies List, Secure Flight may generate a false positive match to the Quiet Skies List. TSA has mitigated the possibility by adjusting the span of the algorithms used to match passengers. Individuals may also seek redress through DHS TRIP.

Auditing and Accountability

TSA Program officials, Information System Security Officers, and Privacy Office work to ensure compliance with policy and applicable legal authorities, examine whether there are changes planned for the programs, and assess privacy impacts. In addition, TSA requires that its personnel receive mandatory privacy training to ensure their understanding of their obligations under the Privacy Act and this PIA.

Access to Silent Partner information within ATS is limited in accordance with CBP protocols. Access to Quiet Skies information is limited to operational analysts with access controlled by individual username and password, and technical support staff that have been specifically granted access through individual user accounts and passwords. Users also need database access and knowledge on how to manipulate the data.

TSA Chief Counsel's office and Privacy Office review information sharing agreements, Memoranda of Understanding (MOU), and new uses and new access to the system. In addition, TSA conducts annual reviews of the PIA and bi-annual reviews of SORNs to ensure they are still valid and meet authorized information sharing requirements and protocols.

Responsible Officials

Thomas Bush
Assistant Administrator
Intelligence and Analysis
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Chief Privacy Officer (Acting)
Department of Homeland Security