Privacy Impact Assessment Update
for

Secure Flight
DHS/TSA/PIA-018(h)

July 12, 2017

Contact Point
Thomas Bush
Assistant Administrator
Office of Intelligence & Analysis
Transportation Security Administration
SFCommunications@dhs.gov
Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) Secure Flight program screens aviation passengers and certain non-travelers before they access airport sterile areas or board aircraft. This Privacy Impact Assessment (PIA) update reflects: 1) that Secure Flight will share information with U.S. Customs and Border Protection (CBP) on passengers flying over the United States and on international point-to-point flights operated by U.S. air carriers to identify for enhanced screening individuals who present a threat to transportation or national security, including border security, and in furtherance of federal counter-terrorism efforts; 2) that in addition to checking against Terrorist Screening Database watch lists, Secure Flight performs checks against watch lists created under the TSA Administrator's statutory authority ("TSA Watch Lists") to prohibit individuals from entering, or to require individuals to undergo enhanced screening prior to entering, the sterile area or boarding an aircraft; and 3) that TSA will allow airports to use the Secure Flight system to perform watch list checks on workers, inspectors, and others seeking to enter the sterile area for official purposes. Unless otherwise noted, the information provided in previously published PIAs remains in effect. Individuals are encouraged to read all program PIAs to fully understand TSA's privacy assessment of the Secure Flight program.

Introduction

The purpose of the Secure Flight program is to screen individuals before they access airport sterile areas[1] or board aircraft.[2] This screening is designed to identify known or suspected terrorists or other individuals who may be a threat to transportation or national security, to prevent some identified individuals from gaining access to airports and airplanes where they may jeopardize the lives of passengers, and to ensure that other identified individuals receive enhanced physical screening prior to accessing airport sterile areas or boarding an aircraft. Secure Flight compares passenger and non-traveler information to the No Fly and Selectee List components of the Terrorist Screening Database (TSDB)[3] to identify individuals who are known or suspected terrorists and,

[1] "Sterile area" means a portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, an aircraft operator, or a foreign air carrier through the screening of persons and property. 49 C.F.R. §1540.5.
[2] The Secure Flight regulations are found at 49 CFR part 1560. The latest version of the Secure Flight Records System of Records Notice (SORN) was published at 75 FR 18867 (April 13, 2010), and the most recent DHS/TSA/PIA-018(g) Secure Flight Program PIA Update, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-018-g-Secure%20Flight%2C%2020141208.pdf.
[3] The TSDB is maintained by the FBI's Terrorist Screening Center. For additional information about the TSDB, *see* http://www.fbi.gov/about-us/nsb/tsc/tsc_faqs.

when warranted by security considerations, against other watch lists maintained by TSA or other federal agencies.[4]

Secure Flight screening also is designed to identify individuals presenting a lower risk to security for whom expedited screening may be appropriate, allowing TSA to more effectively allocate its screening resources.[5] TSA also uses the Secure Flight program to implement its redress program for individuals who have been assigned a unique redress number by the Department of Homeland Security (DHS) Traveler Redress Inquiry Program.[6] DHS will conduct a Privacy Compliance Review on the Secure Flight program.

Reason for the PIA Update

Sharing Passenger Information with CBP

DHS strives to improve traveler screening and information sharing among DHS components, such as TSA and CBP, to enhance the identification of possible threats and to assist in transportation and national security. Both components receive and review information about airline passengers to determine whether the passengers may access U.S. transportation networks or require additional scrutiny when traveling into or out of the United States.

TSA also receives and reviews information on passengers flying over the United States and passengers traveling on flights between two foreign locations on U.S. aircraft operators that are required to have a full security program.[7] TSA will share Secure Flight passenger data (SFPD) from these flights with CBP, which will use TSA real-time threat-based intelligence scenarios run in CBP's ATS to identify individuals requiring enhanced screening for those flights because they may present threats to transportation or national security, and in furtherance of federal counter-terrorism efforts, as well as to identify individuals posing a significant public health threat. CBP also needs to receive this information to obtain a more comprehensive awareness and understanding of the travel of those individuals who present such threats. This information will permit CBP to identify individuals for additional scrutiny prior to traveling or while crossing U.S.

---

[4] Such other watch lists include the Centers for Disease Control and Prevention (CDC) Do Not Board list for persons who should not be permitted to board an aircraft due to public health concerns, and watch lists derived from real-time threat-based intelligence scenarios created by TSA and run by the U.S. Customs and Border Protection (CBP) Automated Targeting System (ATS) to identify international travelers requiring enhanced screening. For more information on the Automated Targeting System, *see* DHS/CBP/PIA-006(e) Automated Targeting System, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006e-ats-april2017.pdf.

[5] DHS Trusted Traveler Programs, such as the TSA Pre✓® Application Program, are used to vet and identify low-risk travelers. *See* https://www.dhs.gov/trusted-traveler-programs.

[6] *See* http://www.dhs.gov/files/programs/gc_1169673653081.shtm.

[7] *See* 49 C.F.R. parts 1544 and 1546.

borders, which, in turn, will strengthen CBP's inbound and outbound activities in support of its national security, border security, and federal counter-terrorism efforts as set forth in Title IV of the Homeland Security Act of 2002 and related authorities.[8]

TSA Watch Lists

Under the Aviation and Transportation Security Act, Pub. L. 107-71, TSA is responsible for: security in all modes of transportation;[9] screening operations for passenger air transportation;[10] receiving, assessing, and distributing intelligence information related at transportation security;[11] assessing threats to transportation;[12] coordinating countermeasures;[13] and carrying out such other duties relating to transportation security as it considers appropriate.[14] The TSA Administrator may "prevent an individual from boarding an aircraft or take other appropriate action" to mitigate threats to aviation security.[15] The Administrator is further directed to cancel a flight or series of flights if "a decision is made that a particular threat cannot be addressed in a way adequate to ensure, to the extent feasible, the safety of passengers and crew" of the affected flights.[16] Additionally, TSA must ensure that federal agencies "share . . . data on individuals . . . who may pose a risk to transportation or national security," and "establish procedures for notifying the Administrator of the Federal Aviation Administration, appropriate state and local law enforcement officials, and airport or airline security officers of the identity of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety."[17] Pursuant to TSA's Secure Flight Program, aircraft operators are required to collect and transmit certain passenger data for watch list matching purposes including denial of boarding and enhanced screening.[18]

TSA has the authority to require appropriate security measures for airline travelers who are a threat to civil aviation or national security, including preventing an individual from boarding an aircraft, requiring enhanced screening for an individual, alerting security personnel that an individual is expected at the airport or taking other appropriate measures. The lists created under this authority supplement the Terrorist Screening Center's Terrorist Screening Database in two ways. First, the TSA Watch Lists are the mechanism by which TSA may take immediate action to

---

[8] *See* DHS/CBP/PIA-006(e) Automated Targeting System, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006e-ats-april2017.pdf.
[9] 49 U.S.C. § 114(d).
[10] 49 U.S.C. § 114(e).
[11] 49 U.S.C. § 114(f)(1).
[12] 49 U.S.C. § 114(f)(2).
[13] 49 U.S.C. § 114(f)(4).
[14] 49 U.S.C. § 114(f)(15).
[15] 49 U.S.C. § 114(h).
[16] 49 U.S.C. § 44905(b).
[17] 49 U.S.C. § 114(h).
[18] 49 CFR part 1560.

mitigate a threat pending further investigation or TSDB watchlisting action for those individuals who meet the interagency Watchlisting Guidance criterion for inclusion in the TSDB. Second, the TSA Watch Lists are used to mitigate threats to transportation or national security posed by individuals who are not on a TSDB watch list but who nonetheless present a threat to transportation or national security. For example, an individual who repeatedly attempts to evade TSA's screening procedures at an airport checkpoint represents such a threat. The TSA Watch Lists enable the addition of an individual to a watch list, sometimes under time exigent circumstances, used by Secure Flight in the airline passenger screening process to enable TSA to take action commensurate with the threat posed by the individual (*e.g.,* denial of boarding or enhanced physical screening). The vast majority of passengers will not be affected by the TSA Watch List program. While the size of the program may change according to new threats and security incidents, as of July 1, 2017, fewer than 20 individuals were included within this program.

Individuals may be nominated to a TSA Watch List based on intelligence or law enforcement information specific to the individual, or their involvement in a security incident that indicates that they may pose, or are suspected of posing, (1) a threat to transportation or national security, (2) a threat of air piracy or terrorism, (3) a threat to airline or passenger safety or (4) a threat to civil aviation security. Nominations to a TSA Watch List may come from within TSA, from other DHS Components, or from other government agencies (federal, state, local, and international). All additions to a TSA Watch List are approved by the TSA Administrator or his/her designees, and the action memorialized in a memorandum outlining the purpose for the addition. Each addition to a TSA Watch List is reviewed for legal sufficiency. Periodic reviews, including by the TSA Office of Intelligence & Analysis; the Office of Civil Rights & Liberties, Ombudsman, and Traveler Engagement; and the Office of Chief Counsel are conducted to recommend whether the individual should remain on or be removed from a TSA Watch List. All continuations to a TSA Watch List are approved by the TSA Administrator or his/her designees. Reviews generally occur no less frequently than on a quarterly basis and include review of current intelligence and other available information. Individuals may not be added to TSA Watch Lists based solely on an individual's real or perceived race, color, religion, national origin, ethnicity, gender, age, sexual orientation, gender identity or disability. However, this information may be considered under the totality-of-the-circumstances in cases where it is both relevant and based on specific intelligence or threat information. Individuals shall not be added to a TSA Watch List in retaliation for engaging in activities protected by the Constitution. In particular, engaging in First Amendment protected activity shall not be a basis for placement on a TSA Watch List.

Sterile Area Access for Official Purposes

Aircraft operators and airport operators can issue gate passes for non-travelers who seek to enter the sterile area to escort or meet a passenger or for other purposes approved by TSA, such as to shop at commercial establishments located beyond the checkpoint. These non-travelers are

screened against the TSDB and other watch lists to ensure that they do not present a threat to transportation or national security. TSA has expanded the approved purposes for non-traveler access to include aircraft or airport operator permission to allow entry into the sterile area for any official purpose, such as construction, maintenance, and inspection of airport facilities. These non-travelers will be screened against watch lists by airport and aircraft operators that have access to the Secure Flight system via the eSecure Flight portal.

Privacy Impact Analysis

Information Collected and Stored within the System

Sharing Passenger Information with CBP

There is no change since TSA already collects the passenger information that it will provide to CBP.

TSA Watch Lists

The DHS/TSA-019 Secure Flight Records maintains specific information (name, date of birth, gender) from the TSA Watch Lists, but does not retain the other information.

TSA will also retain the results of its assessment of the individual's risk and information supporting the individual's original and, as applicable, continued placement on a TSA Watch List within its DHS/TSA-011 Transportation Security Intelligence Service Operations Files. TSA maintains in those records the following information if available:

- full name and any aliases;
- date of birth;
- gender;
- place of birth;
- citizenship, including immigration status and an alien registration number for both naturalized citizens and aliens (if applicable);
- photograph;
- home address or other contact information;
- border crossings; and
- when applicable, transportation worker credential type and status.

Information in the Intelligence Service Operations Files may be collected from TSA security incidents, and from intelligence and law enforcement information provided by other agencies. Information may also be sourced from commercial sources or publicly available data. TSA uses information from commercial sources or publicly available data to identify residence, employment, or other information relevant to placement on the TSA Watch Lists.

TSA relies on the accuracy of the information maintained within the systems that provide the information. When the source information is a security incident that involved TSA, the information is based on direct TSA employee observation, law enforcement, and reporting by witnesses. When the source information is external to TSA, TSA will evaluate its credibility prior to making its determination regarding placement of an individual on a TSA Watch List, and will routinely monitor reporting regarding the individual to reassess the accuracy of the information supporting placement of the person on a Watch List. All additions to the TSA Watch Lists must be approved by the TSA Administrator or his designees, and the addition must be memorialized in a memorandum outlining the purpose for the addition based upon an assessment of current intelligence or information. Each addition to a TSA Watch List is reviewed for legal sufficiency. Periodic reviews are conducted to determine whether the individual should remain on or be removed from the TSA Watch Lists. All continuations on the TSA Watch Lists must be approved by the TSA Administrator or his designees.

Privacy Risk: There is a risk that nominations from other agencies will be for purposes unrelated to TSA missions.

Mitigation: The risk is mitigated by TSA analyzing the information provided, including conducting additional research, to determine whether the individual no longer poses, or is suspected of posing, (1) a threat to transportation or national security, (2) a threat of air piracy or terrorism; (3) a threat to airline or passenger safety; or (4) a threat to civil aviation security, or until appropriate measures are in place to mitigate the threat. Each addition is reviewed for legal sufficiency and memorialized in a memorandum substantiating the decision with available information. TSA will reject nominations for purposes that fall outside of those listed above.

Privacy Risk: There is a risk that third-party data used to place or maintain an individual on a TSA Watch List may be inaccurate.

Mitigation: The risk is partially mitigated. TSA reviews the underlying derogatory information on each individual, evaluates the credibility of the reporting in conjunction with data from other sources, and makes an independent evaluation on whether the facts support placing the individual on a TSA Watch List. In some instances, however, TSA will rely on the third-party data, such as intelligence reporting, that cannot be independently verified and, due to the nature of the reporting, cannot be verified with the individual.

Sterile Area Access for Official Purposes

There is no change to the Secure Flight program associated with permitting airports and aircraft operators to use the Secure Flight system to perform watch list checks on non-travelers seeking sterile area access for official purposes.

Uses of the System and the Information

Sharing Passenger Information with CBP

Secure Flight information shared with CBP will be used for transportation and national security purposes, including identifying passengers who may require additional airport passenger pre-board screening, and for federal counter-terrorism purposes, as well as to identify individuals posing a significant public health threat.

Privacy Risk: There is a risk that Secure Flight information will be used other than for transportation and national security and support of the federal government's counter-terrorism efforts.

Mitigation: The CBP uses are consistent with the purpose of the Secure Flight system to enhance transportation and national security and support the Federal Government's counter-terrorism efforts. In addition, TSA and CBP have worked together to develop processes and procedures that are designed to ensure the data are used properly. CBP Privacy will conduct a CBP Privacy Evaluation (CPE) within 6 months of CBP beginning regular ingest of the SFPD to verify that CBP is properly using SFPD data. The results of the CPE will be shared with the DHS and TSA Privacy Offices.

TSA Watch Lists

TSA will use the information to determine appropriate security measures for airline travelers, such as enhanced screening for an individual before boarding an aircraft or preventing an individual from boarding an aircraft. Other federal agencies may nominate individuals for inclusion on a TSA Watch List, and the nomination may be approved when the individual meets program criteria for inclusion and such action is consistent with TSA's mission.

Privacy Risk: There is a risk that individuals will be inappropriately placed on a TSA Watch List by TSA.

Mitigation: To mitigate this risk, TSA exercises its best judgment in ensuring that individuals are appropriately placed on a TSA Watch List. Nominations to a TSA Watch List must meet the criteria developed by TSA, in accordance with its statutory authorities to deny boarding or take other appropriate action to ensure the security of aircraft. Each individual addition to the Watch List must be approved by the TSA Administrator or his designees, and the addition memorialized in a memorandum outlining the purpose for the addition based upon an assessment

of current intelligence or derogatory information. Prior to submission to the TSA Administrator or designee for approval, a Federal Security Director or Supervisory Air Marshal in Charge, must review and concur with the request, minimizing the risk that an individual will inappropriately submit a person for inclusion on a TSA Watch List. If the request for addition does not originate from within TSA, TSA will ensure that the request comes from a legitimate source and that a senior supervisor has reviewed the request before the request is made. Additionally, TSA will make its own independent decision about whether the request meets TSA's criteria for inclusion on a TSA Watch List. Each addition to a TSA Watch List is reviewed for legal sufficiency. Further, TSA conducts periodic reviews to determine whether the individual should remain on or be removed from the TSA Watch Lists, based upon an assessment by TSA of whether the individual continues to meet TSA's applicable standards for inclusion on each TSA Watch List. Finally, mitigation may be provided when individuals on a TSA Watch list seek redress through the DHS Traveler Redress Inquiry Program at https://trip.dhs.gov/.

Sterile Area Access for Official Purposes

TSA will use the information collection to permit access to sterile areas for approved purposes. The number of non-traveling individuals seeking access to the sterile area for official purposes is expected to be an extremely small percentage of the roughly 2 million individuals checked daily by Secure Flight.

Retention

Sharing Passenger Information with CBP

Passengers on overflights and international point-to-point flights by U.S. carriers who are not identified as requiring additional scrutiny or as potential risks to transportation or national security or for federal counter-terrorism purposes will have their Secure Flight passenger data deleted within 7 days after the flight itinerary. All other passengers will have their passenger data stored within CBP ATS for up to 15 years in accordance with the ATS retention schedule.

Privacy Risk: There is a risk that Secure Flight passenger data will be stored longer than under the Secure Flight retention schedule.

Mitigation: The risk is partially mitigated by CBP's agreement to delete passenger data within 7 days after the flight itinerary for passengers who do not require additional scrutiny. CBP will retain passenger information for passengers who do require additional scrutiny because they present a risk to transportation or national security or for terrorism for 15 years, which is longer than the Secure Flight retention of 7 years, but shorter than the 30-year retention for passengers who are a confirmed match to a watch list.

TSA Watch Lists

TSA Watch List master files are maintained for 30 years after the date of entry, in accordance with the NARA-approved retention schedule (N1-560-04-12). The records are maintained for use while the individual remains watch listed, as well as for oversight and review purposes.

Privacy Risk: There is a risk that information is retained for longer than necessary.

Mitigation: TSA will retain these records in accordance with the 30-year records retention schedule approved by NARA. While the records will be maintained to meet the NARA approved schedule, the impact to the individual is mitigated by TSA's periodic review of the Watch Lists and removal of individuals from the lists as warranted.

Sterile Area Access for Official Purposes

No change.

Internal Sharing and Disclosure

Sharing Passenger Information with CBP

TSA will share Secure Flight passenger data (name, date of birth, gender, passport information if available, redress number, known traveler number, and flight itinerary) with CBP.

Privacy Risk: TSA will share passenger data with CBP on passengers that CBP does not currently receive.

Mitigation: Sharing passenger data with CBP for transportation and national security and Federal counter-terrorism purposes is consistent with the purposes for which the Secure Flight system is operated, as published in the Secure Flight regulations at 49 CFR Part 1560 and the Secure Flight System of Records Notice. It furthers DHS efforts to share information among its components and improve traveler screening and is consistent with both TSA's and CBP's missions.

TSA Watch Lists

TSA will share TSA Watch List information internally for operational and management purposes as well as for purposes of oversight by the TSA Office of Intelligence & Analysis; the Office of Civil Rights & Liberties, Ombudsman, and Traveler Engagement; and the Office of Chief Counsel. Information on individuals on a TSA Watch List who also hold a transportation security credential issued by TSA will be shared within TSA to evaluate whether the credential should be revoked. The facts underlying placement on the TSA Watch List will be reviewed, but the fact of placement on the TSA Watch List is not a factor in the revocation review. So, for example, an airport badge holder arrested for smuggling weapons through an airport may be added to the TSA

Watch List but only the facts of the underlying conduct by the individual and the arrest would be reviewed for purposes of determining whether the airport badge should be revoked.

Sterile Area Access for Official Purposes

Non-traveler information will be shared internally for purposes of granting or denying access to the sterile area.

External Sharing and Disclosure

Sharing Passenger Information with CBP

No change.

TSA Watch Lists

TSA Watch List information and encounters with the individual may be shared with the Terrorist Screening Center (TSC) as part of TSC's watch list nomination process and to coordinate an interagency operational response. TSA will also share information with agencies that seek to nominate individuals to a TSA Watch List for purposes of coordinating on the nomination and any encounters with the individual.

Sharing with the TSC and nominating agencies is compatible with DHS/TSA-011 TSA Transportation Security Intelligence Service Operations Files system of records notices, through routine use R "to the appropriate federal, state, local, tribal, territorial, or foreign governments, or other appropriate authority, regarding or to identify individuals who pose, or are suspected of posing, a risk to transportation or national security." This is compatible with the collection of information for purposes of intelligence, counterintelligence, transportation security, and to identify potential threats to transportation security, uphold and enforce the law, and ensure public safety. Sharing of this information also is compatible with DHS/TSA-019 Secure Flight system of records routine use "(5) To the appropriate federal, state, local, tribal, territorial, or foreign, agency regarding or to identify individuals who pose, or are under reasonable suspicion of posing a risk to transportation or national security."

Privacy Risk: There is a risk that information will be inappropriately shared.

Mitigation: TSA may share this information in accordance with the Privacy Act. TSA mitigates attendant privacy risk by sharing externally only in accordance with published routine uses under the Privacy Act. Further, TSA has entered into a Memorandum of Understanding (MOU) with the FBI and TSC governing the conditions of sharing information.

Privacy Risk: There is a risk that other agencies will use a TSA Watch List for their own purposes to the detriment of the individual.

Mitigation: This risk is partially mitigated by TSA's active coordination with other agencies and its sharing only pursuant to a published routine use, and as further specified in the MOU with the FBI and TSC. TSA shares information regarding upcoming expected encounters with TSA Watch List subjects with the TSC (and within DHS to coordinate an operational response). When an individual on a TSA Watch List is encountered, TSA may provide the basis for watch listing and associated derogatory information to non-DHS agencies to provide these agencies with context as to why TSA has identified the individual for a denial of boarding or other security measure. This information is provided so that the non-DHS agencies may determine whether additional action is warranted and appropriate under their own authorities and policies. Additionally, all inclusions on a TSA Watch List, including those from non-DHS agencies, are reviewed and vetted by TSA personnel before an individual is added to ensure that each person included on a TSA Watch List meets the applicable standard for inclusion.

Sterile Area Access for Official Purposes

TSA will disclose a sterile area admission decision to the airport or aircraft operator sponsoring the individual seeking access for official purposes.

Notice

Sharing Passenger Information with CBP

No change.

TSA Watch Lists

In general, TSA will not provide notice of the collection of information to an individual of his or her placement on the TSA Watch List. When TSA receives personal information as part of suspicious activity reports, the individual is unlikely to have knowledge that his/her information has been submitted to TSA and there is no opportunity for TSA to provide notice. TSA also receives some of the information from other agencies and does not provide notice that it received such information to individuals. Such notice may compromise the intelligence or law enforcement efforts underlying the placement of the individual on the TSA Watch List. TSA may provide notice of the collection of information for individuals involved in a security incident, including via DHS/TSA-001, Transportation Security Enforcement Record System, and DHS/TSA-011, Transportation Security Intelligence Service Operational Files.

Privacy Risk: There is a risk that individuals may be unaware that they are on a TSA Watch List.

Mitigation: This risk is partially mitigated through the publication of this PIA, which provides a description of the types of individuals who may appear on a TSA Watch List and outlines the Watch List's intended purpose. Because the TSA Watch Lists are used for security

purposes, generally, notice or the opportunity to consent to use of the information would compromise the underlying purpose of the system. In addition, TSA receives some of the information from other agencies and may not provide notice to individuals in question without compromising ongoing law enforcement or intelligence matters. Individuals who believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at an airport may apply for redress with the Department of Homeland Security Traveler Redress Inquiry Program at https://trip.dhs.gov/.

Sterile Area Access for Official Purposes

No change. Non-traveling individuals seeking access to the sterile area for official purposes will be provided the same notice as other non-traveling individuals seeking access to the sterile area.

Individual Access, Redress, and Correction

Sharing Passenger Information with CBP

No change.

TSA Watch Lists

Individuals may request access to their data under the Privacy Act or the Freedom of Information Act by contacting the TSA Headquarters Freedom of Information Act (FOIA) Office, at FOIA Officer, Transportation Security Administration, TSA-20, Arlington, VA 20598-6020. Access may be limited pursuant to exemptions asserted under 5 U.S.C. § 552a(j)(2), (k)(1), and (k)(2). In addition, section 14 of Executive Order 13768 may restrict the application of the Privacy Act for certain persons.

Privacy Risk: There is a risk that individuals will not have an opportunity to correct, access, or amend their records maintained by TSA.

Mitigation: Individuals may seek access to TSA records by submitting a request under the Privacy Act, though some aspects of their record may be exempt from access, or may otherwise be limited pursuant to EO 13768 In addition, individuals who believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at an airport, regardless of immigration status, may seek redress through the DHS TRIP program.

Sterile Area Access for Official Purposes

No change.

Technical Access and Security

Sharing Passenger Information with CBP

No change.

TSA Watch Lists

No change. Existing watch list processes are applied to the TSA Watch Lists.

Sterile Area Access for Official Purposes

No change.

Technology

Sharing Passenger Information with CBP

No change.

TSA Watch Lists

No change.

Sterile Area Access for Official Purposes

No change.

Responsible Officials

Thomas Bush
Assistant Administrator
Office of 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
Acting Chief Privacy Officer
Department of Homeland Security