



**Privacy Impact Assessment Update
for**

Secure Flight

DHS/TSA/PIA-018(g)

December 08, 2014

Contact Point

David P. Harding

Office of Strategy and Mission Support Branch

Transportation Security Administration

SFCommunications@dhs.gov

Reviewing Official

Karen L. Neuman

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 the incorporation of risk-based assessments generated by aircraft operators using data in their existing Computer-Assisted Passenger Prescreening Systems (CAPPS). CAPPS assessments are used in risk-based analysis of Secure Flight and other prescreening data that produce a boarding pass printing result for each passenger. In addition, the update reflects that Secure Flight incorporates checks against watch lists of lost and stolen travel documents, including international passports. This PIA update also reflects the addition of records of TSA and DHS employees who have opted-in to TSA Pre✓[®] as another known traveler population stored by Secure Flight. 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 areas¹ or board aircraft.² Generally, this screening is designed to identify and prevent known or suspected terrorists or other individuals from gaining access to airports and airplanes where they may jeopardize the lives of passengers and others. TSA uses the Secure Flight program to compare passenger and non-traveler information to the No Fly and Selectee List components of the Terrorist Screening Database (TSDB)³ to identify those who present a threat to aviation security and, when warranted by security considerations, against other watch lists maintained by TSA or other federal agencies.

More recently, Secure Flight has also been used to identify individuals presenting a lower risk to security, allowing TSA to more effectively allocate its screening resources. As discussed in the September 4, 2013 PIA Update, Secure Flight uses passenger reservation information for a flight by flight risk assessment to determine the appropriate level of screening, including expedited screening. Passengers who are eligible for expedited screening are referred to a TSA Pre✓[®] lane where they typically will be able to leave on their shoes, light outerwear, and belt,

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 In October 2008, TSA published the Secure Flight Final Rule (73 FR 64018, Oct. 28, 2008) and the related PIA (Secure Flight Program PIA Update – DHS/TSA/PIA-018(a) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_secureflight2008.pdf).

³ For additional information about the TSDB, see http://www.fbi.gov/about-us/nsb/tsc/tsc_faqs.



to keep their laptop in its case, and to keep their 3-1-1 compliant liquids/gels bag in a carry-on. TSA Pre✓® lanes are available at more than 118 airports nationwide.⁴

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.⁵

Reason for the PIA Update

Background on CAPPS

This PIA update reflects the use of the Computer-Assisted Passenger Prescreening System (CAPPS) to incorporate aircraft operator-generated CAPPS assessments into the Secure Flight risk assessment. The Federal Aviation Administration created CAPPS in 1999 in order to “exclude from the additional security measures the great majority of passengers who are very unlikely to present any threat and, conversely, to identify passengers to whom heightened security measures should be applied.”⁶ The FAA implemented CAPPS pursuant to its general authority to prescribe regulations “to protect passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy.”⁷ Using FAA-set evaluation criteria to determine a passenger’s security risk, CAPPS was run by aircraft operators in their reservation systems and analyzed passenger name records (PNR)⁸ and other information associated with flight reservations to determine a passenger’s security risk prior to boarding.

TSA was created in 2001 with the enactment of the Aviation and Transportation Security Act (ATSA),⁹ and assumed responsibility for the CAPPS program from the FAA.¹⁰ CAPPS

⁴ See <http://www.tsa.gov/tsa-precheck/airlines-airports>.

⁵ See http://www.dhs.gov/files/programs/gc_1169673653081.shtm.

⁶ See FAA Notice of Proposed Rulemaking, Security of Checked Baggage on Flights Within the United States, 64 FR 19220, 19221 (April 19, 1999).

⁷ See 49 U.S.C. § 44903(b).

⁸ A PNR is a record that contains detailed information about an individual's travel on a particular flight, including information provided by the individual when making the flight reservation. Although the content of PNRs varies by aircraft operator, PNRs may include, among other information, passenger name, reservation date, travel agency or agent, travel itinerary information, form of payment, flight number, and seating location.

⁹ Pub. L. 107–71, 115 STAT. 597 (Nov. 19, 2001).

¹⁰ In section 136 of ATSA (codified at 49 U.S.C. 44903(j)(2)(C)), Congress directed that aircraft operators use CAPPS or any successor system to screen all aircraft passengers, not just those who are checking bags. See also TSA Notice of rulemaking status, Security of Checked Baggage on Flights Within the United States; Certification of Screening Companies, 67 FR 67382, 67383 (Nov. 5, 2002). In addition, ATSA continued in effect all “orders, determinations, rules, [and] regulations” of the FAA “until modified, terminated, superseded, set aside, or revoked in accordance with law by the [TSA Administrator], any other authorized official, a court of competent jurisdiction, or operation of law.” See ATSA, section 141(b). ATSA also explicitly recognized the continuance of CAPPS when it exempted CAPPS from the requirement that the screening of passengers and property before boarding flights



continued to be operated by U.S. aircraft operators pursuant to the TSA-mandated Aircraft Operator Standard Security Program (AOSSP). Under this program, and prior to the implementation of Secure Flight, airlines were required to check passenger reservation data against watch lists. A CAPPS assessment indicating risk above a pre-set threshold required enhanced screening for passengers who were not on a watch list. The aircraft operator would add the additional screening instruction to the boarding pass and TSA would perform the additional screening for those passengers requiring additional screening as a result of their CAPPS assessment. As with the FAA, TSA did not receive the underlying PNR and associated reservations information. The additional screening included enhanced physical searches of individuals and their carry-on bags at the checkpoint.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) was enacted in December 2004.¹¹ Section 4012(a)(1)-(2) of IRPTA directs TSA and DHS to assume the function of comparing aircraft operator passenger information to data in the TSDB maintained by the Terrorist Screening Center from aircraft operators. Consistent with this statutory directive, TSA promulgated its Secure Flight Program regulations.¹² By November 2010, TSA fully assumed the watch list matching function from aircraft operators and air carriers in Secure Flight. Since that time CAPPSS has not been used to determine whether additional screening is warranted for certain passengers. Notably, however, IRTPA did not remove or amend the statutory requirement for aircraft operators to use CAPPSS. Accordingly, the statutory and regulatory authorities for the use of CAPPSS remain.

Use of CAPPSS Assessments in Secure Flight Risk-Based Analysis

TSA plans to incorporate the CAPPSS assessment generated by aircraft operators into its Secure Flight risk-based analysis of passenger and other prescreening data as part of TSA's ongoing efforts to enhance aviation security by identifying appropriate security screening for aviation travelers. The CAPPSS assessments are designed to enhance TSA's analysis of passenger security risk and to enable TSA to make better passenger risk decisions. The incorporation of a CAPPSS assessment into the Secure Flight risk-based analysis program, with

originating in the United States be carried out by a Federal Government employee. See 49 USC 44901(a).

¹¹ Pub. L. 108-458, 118 Stat. 3638 (December 17, 2004). A genesis for IRPTA was the report of the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), which recommended that TSA perform watch list matching using the "larger set of watch lists maintained by the Federal Government," and that screening issues associated with CAPPSS be elevated for high-level attention and addressed promptly by the government. See Final Report of the National Commission on Terrorist Attacks Upon the United States, page 393 (July 22, 2004).

¹² 73 FR 64018 (Oct. 28, 2008).



Secure Flight Passenger Data (SFPD)¹³ and other prescreening data, is consistent Congress's direction in ATSA to use CAPPs in passenger screening.

CAPPs assessments generated by aircraft operators continue to rely on information collected by those operators in the ordinary course of business. Secure Flight does not receive the underlying data that are used for the CAPPs assessment. By receiving a CAPPs assessment TSA obtains important security value from information without receiving all the underlying data that are generated when individuals make their flight reservations.

TSA has taken a number of steps to review the security value of CAPPs data including evaluating whether certain CAPPs data are indicative of low-risk passengers. First, TSA worked with its airline partners to re-assess the security value of the individual CAPPs data elements. This effort resulted in refining CAPPs data elements. Second, TSA engaged the Civil Aviation Threat Working Group (CATWG), which is composed of analysts from various Federal Government agencies and led by a representative from the National Counterterrorism Center, to provide its assessment of the security value of CAPPs data. The CATWG provided its report of findings and recommendations in September 2013, which further refined the security value assigned to CAPPs data elements. Third, TSA asked the Homeland Security Studies and Analysis Institute (a federally-funded research and development center) to review its approach to risk-based security screening, including the use of CAPPs assessments. In March 2014, the Institute endorsed TSA's approach for conducting Secure Flight risk-based analysis and recommended that TSA continue to strengthen this analysis by including CAPPs assessments. Finally, TSA reviewed its plans to use CAPPs assessments with senior officials from the Department of Homeland Security Offices of Privacy, Civil Rights and Liberties, and General Counsel. TSA further refined the security value assigned to CAPPs data elements based on input from these offices. These offices found that CAPPs assessments may be used as part of the Secure Flight risk-based analysis while also protecting passengers' privacy, civil rights, and civil liberties. In addition, these DHS offices will review CAPPs operations on an on-going basis, including the risk value assigned to individual CAPPs data elements, to assure CAPPs's continued security value, its connection to evolving security threat information, and its adherence to privacy, civil rights, civil liberties, and legal principles.

Currently, the Secure Flight passenger prescreening system has watch lists of high-risk individuals and uses these lists to issue boarding pass printing results, e.g., selectee screening or do not board instructions. TSA also has lists of low-risk individuals who have been issued known traveler numbers (KTN) by TSA, who are eligible for expedited screening. These

¹³ SFPD consists of name, gender, date of birth, passport information (if available), redress number (if available), known traveler number (if available), reservation control number, record sequence number, record type, passenger update indicator, traveler reference number, and itinerary information.



individuals may receive a boarding pass printing instruction that enables them to use TSA Pre[✓][®] lanes. TSA also uses risk-based analysis of SFPD and other prescreening data to make screening determinations (e.g., to determine whether a passenger is eligible for expedited screening).¹⁴ The addition of CAPPS assessments to existing Secure Flight risk-based analysis will strengthen the risk assessment and increase the confidence level in the determination that a passenger is a lower-risk and eligible for expedited screening. The level of screening for a passenger may change from flight to flight based on the particulars of a flight or the individual. CAPPS is expected to result in more passengers receiving expedited screening, however, CAPPS assessments could lead to people receiving enhanced screening.

After these changes are implemented, passengers who are a match to a watch list will continue to receive appropriate enhanced screening. For all other passengers, the Secure Flight passenger prescreening computer system conducts risk-based analysis using, among other data: 1) the SFPD (including KTN) that TSA already receives from aircraft operators pursuant to Secure Flight regulations; 2) the CAPPS assessments; 3) frequent flyer designator codes that aircraft operators submit to TSA; and 4) other prescreening data available to TSA. The Secure Flight risk-based analysis determines whether passengers receive expedited, standard, or enhanced screening, and the results are indicated on the passenger's boarding pass.

No one will be denied the ability to fly or to enter the sterile area of an airport based solely on the results of the Secure Flight risk-based analysis, including the use of a CAPPS assessment in that analysis.

The rules-based analysis includes a level of randomness to ensure unpredictable results. One potential result of the randomness rules is that a passenger who otherwise would have received expedited screening may instead be randomly selected to receive standard screening or enhanced screening, such as explosives detection testing.

Other Updates

This PIA update also reflects that TSA now checks passenger reservation data including passport information against watch lists of lost and stolen travel documents, including international passports. Passengers using lost or stolen travel documents will not be permitted to fly. Finally, this update also reflects the addition of records of TSA employees who have opted-in to TSA Pre[✓][®] as another known traveler population stored within the Secure Flight system, and the expected addition of DHS employees who have similarly opted-in to the program.

¹⁴ For a discussion of Secure Flight risk-based analysis, see the September 10, 2013 Secure Flight SORN update at 78 FR 55270, and the Privacy Impact Assessment for Secure Flight, DHS/TSA/PIA-018(f) (Sept. 4, 2013), found at <http://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa-secure-flight-update-09042013.pdf>



Privacy Impact Analysis

Information Collected and Stored within the System

TSA receives the CAPPS assessment from the aircraft operator when it transmits passenger SFPD to TSA. It is stored within Secure Flight with the passenger's record in accordance with the NARA approved records retention schedule. For the vast majority of passengers, such records are deleted within seven days after directional travel has been completed. Directional travel means each direction of a round trip itinerary will be assessed separately.

Secure Flight will also store the name, gender, date of birth, and KTN of TSA and DHS employees who have opted-in to TSA Pre✓[®].

Privacy Risk: There is a risk that TSA receives additional passenger data for Secure Flight from the PNR and reservations data used by CAPPS.

Mitigation: The risk is mitigated by having the CAPPS assessment performed by the aircraft operator using data already received by them in the normal course of business.

Uses of the System and the Information

TSA uses the information collected by Secure Flight to issue an appropriate boarding pass instruction for screening. TSA incorporates CAPPS risk assessments into its passenger prescreening system. These numerical risk assessments are designed to further refine TSA analysis of passenger security risk and enable TSA to make better passenger risk decisions, primarily to identify passengers who are eligible for expedited screening in airports with TSA Pre✓[®] lanes, but also for enhanced screening. The incorporation of CAPPS into TSA's computerized passenger prescreening system, along with SFPD, is consistent with the direction from Congress in ATSA to use CAPPS in passenger screening. TSA will not receive the underlying PNR and other data collected by aircraft operators in their ordinary course of business that is analyzed by CAPPS, but instead will receive a CAPPS assessment for each individual.¹⁵

Secure Flight checks lost and stolen travel document watch lists to identify passengers using such documents and to prohibit them from boarding covered aircraft. Secure Flight uses the list of TSA and DHS employees who have opted-in to TSA Pre✓[®] to confirm eligibility for

¹⁵ TSA, however, remains authorized to obtain such information for transportation security purposes under TSA's general compliance and enforcement authorities, such as TSA's authority to inspect aircraft operators to ensure compliance with security programs and TSA regulations (49 U.S.C. § 114(f)(7), 49 C.F.R. § 1544.3); and TSA's authority to issue subpoenas and orders for the production of information (49 U.S.C. §§ 40113(a) and 46104, 49 C.F.R. 503.203(a)). TSA also continues to receive SFPD required under the Secure Flight rulemaking.



expedited screening when the individual makes a reservation.

Privacy Risk: There is a risk that incorporating CAPPs into Secure Flight may result in a passenger's boarding pass instruction being changed.

Mitigation: The risk is mitigated because CAPPs is a statutorily mandated program that is operated by aircraft operators under TSA authority whether it is part of Secure Flight or not. Furthermore, passenger's instructions should not change unless they are selected for enhanced screening.

Privacy Risk: There is a risk that TSA or DHS employees will have their PII stored within Secure Flight as a known traveler without notice or permission.

Mitigation: The risk is mitigated because TSA and DHS employees are required to expressly opt-in to the program in order to be included.

Retention

No change. The Secure Flight records retention schedule is predicated on the watch list match status and is not affected by CAPPs. Records of passengers who are not a match to a watch list are retained for no more than seven days.

Internal Sharing and Disclosure

No change.

External Sharing and Disclosure

Secure Flight discloses the passport number and country of issuance to the federal and international agencies maintaining lost and stolen travel document watch lists in order to accomplish the check of those lists. In addition, when there is a match to a watch list, TSA provides SFPD to those agencies with investigative or enforcement roles for the watch lists.

Privacy Risk: There is a risk that associated PII may be shared with Agencies that should not receive the PII or that are not responsible for checking whether a passenger has submitted a travel document that has been reported as lost or stolen.

Mitigation: The risk is mitigated because TSA only provides PII to agencies maintaining lists of lost or stolen travel documents when there is a match to such lists.

Notice

No change.



Individual Access, Redress, and Correction

No change.

Technical Access and Security

No change.

Technology

No change.

Responsible Official

David P. Harding
Office of Strategy and Mission Support Branch
Office of Intelligence and Analysis
Transportation Security Administration
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security