Privacy Impact Assessment

for the

Travel Document Checker Automation Using Facial Identification

DHS Reference No. DHS/TSA/PIA-046(d)

Homeland Security

November 17, 2022
(***updated note: November 28, 2023***)

Abstract

The Transportation Security Administration (TSA), in partnership with U.S. Customs and Border Protection (CBP), is expanding the use of facial identification technology to enhance the identity verification process at TSA checkpoints. TSA's latest proof of concept employs a Credential Authentication Technology (CAT) device equipped with a camera (referred to as CAT-2),[1] along with biometric matching services provided by CBP's Traveler Verification Service (TVS),[2] to verify the identities of certain travelers who opt-in during check-in at the Detroit Metropolitan Wayne County Airport (DTW) in partnership with Delta Airlines.[3] This PIA update reflects expanding this concept to additional locations and airlines,[4] and that participating passengers will no longer be required to scan their identity document as part of the proof of concept.

Updated Note: (November 28, 2023): In addition to the Credential Authentication Technology (CAT) devices equipped with a camera (referred to as CAT-2) TSA has deployed for this proof of concept, TSA may also use alternate devices, such as tablets, in lieu of CAT-2 at some airports to test TSA's capability to perform CAT-2 functions. These devices are configured to operate in the same way as CAT-2. There are no other updates to this Privacy Impact Assessment. The descriptions of the Fair Information Practice Principles (FIPPs), privacy risks, and mitigation measures are the same as published on November 22, 2022.

Overview

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. TSA aviation authorities extend to all passengers, regardless of citizenship, for both domestic and international flights, as well as individuals seeking to enter the sterile areas[5] of airports. As part of its efforts to secure aviation transportation, TSA verifies passenger identities before granting access to airport sterile areas. Typically, the TSA Transportation Security Officer (TSO) performing Travel Document Checker (TDC) functions at

[1] CAT-2 has previously been referred to in TSA Privacy Impact Assessments as CAT-C (CAT with a camera). CAT-2 has the capability for the passenger to self-initiate a transaction.
[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACTASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR TDC AUTOMATION USING FACIAL VERIFICATION, DHS/TSA/PIA-046(c), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[4] TSA will publish specific airlines and deployment locations through the TSA website. *See* https://www.tsa.gov/biometrics-technology.
[5] "Sterile areas" are portions of airports that provide passengers access to boarding aircraft and to which the access is generally controlled by TSA, by an aircraft operator, or foreign air carrier through the screening of persons and property (49 CFR Part 1540.5).

the checkpoint verifies a passenger's identity by visually comparing the photograph on the passenger's identity document to the passenger's face, and then comparing the document's biographic information with the biographic information on the passenger's boarding pass.[6] Once those steps are successfully completed, the passenger proceeds to security screening.

In order to improve airport security and expedite the identity verification process, TSA has been exploring the use of biometric matching technologies, with a focus on facial identification as the primary means of identity verification for aviation security screening. In previous proofs of concept, TSA demonstrated the ability to use CAT-2 devices and connections through TSA's Security Technology Integrated Program (STIP)[7] to the TSA Secure Flight system[8] to enhance security and generate boarding pass instructions. TSA transmitted a subset of the following Secure Flight Passenger Data (SFPD) for passengers traveling that day at that airport to CAT-2 devices at security checkpoints via TSA's Secure Technology Infrastructure Program (STIP) system:

- Passengers' full name
- Gender
- Date of birth (DOB), as self-reported when the reservation was made
- Passport information (if available)
- Itinerary information (flight number, departure/arrival airports and times)
- Known traveler number (KTN) (if available)
- Passenger record locator
- Reservation status
- Assigned boarding pass printing result
- Record sequencing/versioning information

Data collected during this proof of concept will be shared with S&T for subsequent qualitative and quantitative analysis.

TSA continues to develop its biometric proofs of concept that rely on a 1:1[9] match of

[6] For passengers who are unable to present verifying identity documentation, TSA offers an alternative identity verification process in which passengers answer knowledge-based questions.
[7] STIP is a suite of TSA applications that provide equipment connectivity, data collection, and data reporting.
[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR SECURE FLIGHT, DHS/TSA/PIA-018, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[9] 1:1 refers to a direct match verification between feature data in the photo of the person presenting themselves at the TDC and the photo on the identity document.

identity against an authenticated identity document that is presented to the TDC.[10] At the same time, TSA is also continuing it development of a 1:n[11] match proof of concept with CBP TVS by expanding to additional airports beyond DTW and airlines beyond Delta. The expanded locations use the same procedures set out in the previous PIA[12], with a single procedural change that participating passengers will no longer be required to scan their identity document at the checkpoint.

Process

As explained in the previous PIA, eligible passengers will make their flight reservation as they normally would. In some instances, this will include submission of a passport number, either by the individual or by the airline holding the passport number, within their passenger profile for submission to the TSA Secure Flight system. When checking in using the airline's mobile application, passengers will be prompted to choose whether to participate in this proof of concept and to provide their passport number if they have not yet done so. For passengers who opt-in, TSA will communicate that choice through technical infrastructure from Secure Flight to CBP TVS to coordinate the TVS query of DHS holdings, stage their templates of previously-acquired images for matching, and send consolidated results to the TDC. TSA and CBP will not access or use biometric information from passengers who do not provide their consent. Passengers will be issued a mobile boarding pass bearing a consent indicator, and an airline representative will review travelers' boarding passes to ensure that only consenting travelers will enter the queue for the proof of concept.

Using the camera device, TSA will collect name, date of birth, and gender from the identity document. TSA will then compare this information to the passenger's SFPD provided during the reservation. In addition, TSA will collect a live photograph of the passenger and transmit it, along with the passenger's passport number, passport country, flight information, known traveler number, and unique identifier to CBP TVS. Once the photograph is received in TVS, it will be converted into a template and matched against a gallery of templates for travelers who opted-in and are traveling from the airport that day. CBP TVS match results will be correlated and transmitted to equipment at the checkpoint to display the newly captured image, along with the traveler's biographic data (full name, date of birth, and Secure Flight vetting status), for the TSO's review. The TSO will receive the result of this matching process on TSA-owned equipment at the screening podium. If the TSO is satisfied there is a match, the passenger will be directed to proceed to security screening. If not, the TSO will follow manual resolution processes to verify

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR TDC AUTOMATION USING FACIAL VERIFICATION, DHS/TSA/PIA-046(b), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[11] 1:n or "1 to many" refers to matching the feature data in the photo of the person presenting themselves at the TDC against a gallery of many previously identified photographs.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR TDC AUTOMATION USING FACIAL VERIFICATION, DHS/TSA/PIA-046(c), *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

the traveler's identity. The match result is displayed until the TSO clears the screen for the next passenger.

TSA will share name, date of birth, gender, identification type, state of issuance, identification number, as well as the live photograph, and the top identity matches with S&T to evaluate the system's ability to make a valid match against the gallery of photographs provided by CBP TVS. Finally, TSA will also collect certain transactional metadata (e.g., transaction ID, timestamps, and quality scores) and outcomes of each transaction (match or no match) for analysis.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[13] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[14]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[15] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[16] and the Homeland Security Act of 2002, Section 222.[17] This PIA examines the privacy impact of this technology proof of concept as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

Passengers must take multiple steps to opt-in to this proof of concept, including affirmative steps during their check-in process and during photograph capture. During check-in, passengers

[13] 5 U.S.C. § 552a.
[14] 6 U.S.C. § 142(a)(2).
[15] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[16] 44 U.S.C. § 3501 note.
[17] 6 U.S.C. § 142.

will opt-in and consent to providing PII to pre-stage their photograph and confirm that they have read a Privacy Notice. TSA provides signage in close proximity to the queue at the airport to provide notice to passengers that taking their photograph is optional and that they can decide not to participate in the pilot by not taking their photograph. Signs at the checkpoint will also provide information regarding the procedures for participating, as well as notice that if passengers choose to have their photo taken, TSA will temporarily save it, along with limited biographic information, to evaluate the technology's effectiveness. Only those passengers who have provided consent will have an opportunity to have their photograph taken. If a passenger declines the live photograph capture, they will be directed to standard screening processing. TSA's strategic communications and public affairs will work to provide information in advance to the public. In addition, this PIA provides notice by publication on a publicly available DHS website.

Privacy Risk: There is a risk that passengers will not know that TSA is taking their photographs for identity verification.

Mitigation: This risk is mitigated. The check-in process requires proactive actions on the part of the passenger to take the photograph at check-in. The consenting passenger must provide a passport number and then pose for the live photo in front of the camera. TSA provides signage indicating which queue is designated for use by participating passengers. At any time before their photo is captured, the passenger may choose to decline the photo capture and request standard security screening and processing. TSA also posts signs in close proximity to the TDC screening podium providing instructions for participating, as well as notification that taking the photograph is optional, and that alternative procedures are available to those who do not wish to participate. In addition, this PIA and public communications materials inform members of the public about the procedures for participating in the proof of concept.

Privacy Risk: There is a risk that the individual may not know that his or her information is being collected and retained by TSA, CBP, and S&T.

Mitigation: This risk is mitigated. Passengers receive notice of this proof of concept when they check-in on the airline's website or mobile application, as well as via signage prior to the security checkpoint and at TSA.gov. In addition, this PIA provides extensive information regarding the role of each agency and partners in this proof of concept.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

This proof of concept requires significant participation by the individual to opt-in, including

during the reservations process, check-in, and at the checkpoint with the TDC. Individuals will have to expressly opt-in during the online check-in process with the airline in order for the photograph to be staged within CBP TVS. Signs in close proximity to the queue will provide notice to passengers about how to participate and the option to decline at any time prior to photo capture. If a passenger declines the live photograph capture, they will be directed to manual processing.

Individuals have previously granted consent to the use of their information provided to Secure Flight during the airline reservation process for security purposes and to generate an appropriate boarding pass instruction. Linking Secure Flight to the TDC permits TSA to provide an appropriate boarding pass instruction at the checkpoint.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The principal purpose of using passengers' PII is to perform identity verification, however this proof of concept also assesses operational and technological components using CBP TVS to stage and match passenger photographs. The Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, provides TSA with broad authority to secure aviation transportation and specifically authorizes TSA to test new technology and equipment.[18] In ATSA, Congress gave TSA specific authority to use biometric and other technologies to prevent persons who may pose a danger to aviation safety or security from boarding an aircraft.[19] TSA has the authority to establish pilot programs to test new technology to ensure safety and security for the airport, including biometric technology that ensures only authorized access to secure areas.[20] In addition, the agency has authority to strengthen access control points by deploying biometric or similar technologies in order to ensure security of passengers and aircraft.[21] Under ATSA, Congress granted TSA with the following responsibilities: security in all modes of transportation; screening operations for passenger air transportation; receiving, assessing, and distributing intelligence information related to transportation security; assessing threats to transportation; coordinating countermeasures; and carrying out such other duties relating to transportation security as it considers appropriate.[22] Finally, the TSA Modernization Act requires a report that includes specific assessments from CBP and TSA regarding the impacts of the use of biometric technology.[23]

4. Principle of Data Minimization

[18] 49 U.S.C. § 114(f)(8), (9).
[19] Pub. L. 107-71, § 109(a)(7) (November 19, 2001) (codified at 49 U.S.C. § 114 note).
[20] 49 U.S.C. § 44903(c)(2)(3).
[21] 49 U.S.C. § 44903(g)(2)(G).
[22] 49 U.S.C. § 114(d)-(f)(15).
[23] TSA Modernization Act, Pub. L. 115-254, § 1919(c) (October 5, 2018).

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

TSA collects only the PII that is directly relevant and necessary to perform identity verification, and to assess critical operational and technological components of the biometric matching. TSA collects the following data:

- Facial images
- Biographic information (name, gender, DOB)
- Passport information
- KTN
- Departure airport/time
- Identification type/state of issuance
- Certain transactional metadata (e.g., transaction ID, timestamps, quality scores)
- Outcomes of each transaction (match or no match) only from passengers who volunteer to participate

TSA shares only passport information, KTN, live photo, name, gender, date of birth, and departure airport/time with CBP TVS. Additionally, TSA minimizes the collection of PII by limiting Secure Flight data that is passed on to the TDC checkpoint to only the local Secure Flight data for that specific airport.

TSA shares the following data collected during the proof of concept with S&T for analysis:

- Name
- DOB
- Gender
- Identification type/state of issuance
- Identification number, as well as the live photograph and the top identity matches (to evaluate the system's ability to make a valid match against photographs in the gallery)

S&T deletes the data no later than 180 days following receipt in accordance with an approved TSA record retention schedule (N1-560-04-14, Item 2). S&T continually evaluates the performance of the camera system (e.g., failure to acquire rate) and system matching performance (e.g., false match rate, false non-match rate). TSA uses the results of this evaluation to identify and

mitigate any performance issues and operational concerns and to inform future expansion of TSA's biometrics development and deployments.

Privacy Risk: There is a risk that TSA will retain passenger information longer than is necessary.

Mitigation: This risk is mitigated. When the TSO at the TDC podium either acknowledges the results or begins the next passenger's transaction, the camera device deletes transactional metadata and biographic information. TSA immediately purges the following from the technical infrastructure communicating with CBP TVS:

- Name
- Gender
- DOB
- Flight information
- Vetting status
- SFPD
- Biometric match/no-match response
- Matching unique identifiers
- Passport information (passport number, passport country, passport expiration date)
- Passenger photographs captured using the camera device (within 24 hours after a passenger's scheduled departure)

PII from Secure Flight will be retained by the technical infrastructure for no longer than 24 hours after the flight departure time to accommodate passengers that may require rescreening due to security events or when they decide to leave the sterile area for various reasons prior to their flight. PII sent back to Secure Flight will follow Secure Flight's retention policy.

During the proof of concept evaluation, S&T deletes the data in no more than 180 days in accordance with TSA's applicable records retention schedule.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Passenger photograph and passport information will be used for the purpose specified above: to verify identity, test system functionality, determine the ability to compare accurately a

passenger's facial image against a gallery of photos from CBP TVS, and incorporate passenger Secure Flight information for display at the checkpoint. Information is shared with CBP for purposes of staging a gallery of passenger photographs and matching a live photograph against the gallery, and with DHS S&T for analysis. Information in Secure Flight is shared in accordance with the Privacy Act, 5 U.S.C. § 552a and per the Routine Uses set forth in DHS/TSA-019 Secure Flight Records.[24]

Privacy Risk: There is a risk that the biometric data will be used for a purpose other than identity verification.

Mitigation: This risk is mitigated. TSA only uses the biometric data to perform identity verification at the checkpoint, and to assess critical operational and technological components of this proof of concept. CBP TVS is only used for identity verification. This proof of concept is only available to passengers who are enrolled in TSA PreCheck® who have a U.S. passport. Thus passenger information that is shared with CBP for purposes of the proof of concept does not create the risk of an immigration enforcement action.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

The PII submitted by the passenger is assumed to be accurate but may be incorrect (typically from a typographical error). Submission of incorrect passport information may prevent correct staging of the gallery within CBP TVS. In other respects, the PII collected during this proof of concept is the same as otherwise collected during normal TSA aviation passenger operations. If the CBP TVS gallery provides multiple potential photograph matches, the TDC will manually select the most accurate. If no match is made, the passenger may undergo a manual resolution of their identity in accordance with standard TSA procedures.

Privacy Risk: There is a risk that the facial images collected through and matched within CBP's TVS System will be lower quality or may not be an accurate representation of the traveler, thus negatively impacting the reliability of the matching service.

Mitigation: This risk is mitigated. CBP and TSA continually test and evaluate the accuracy of the camera technology and the algorithms used for matching. Prior to deploying any modification to the technology or the process, CBP and TSA conduct tests to assess impacts to the traveler and the accuracy of the information to eliminate any adverse impacts. CBP and TSA are also partnering with S&T to evaluate algorithms and test biometric technologies developed by specified vendors.

[24] *See* DHS/TSA-019 Secure Flight Records, 80 Fed. Reg. 233, (January 5, 2015).

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

TSA limits authorized users of the checkpoint hardware used in this proof of concept to the TSA personnel staffing the device. The hardware is physically locked when not in use, and access to the government-furnished computer requires multi-factor authentication, including login with an active Personal Identity Verification (PIV) card and personal identification number (PIN). The information displayed to the TSO is cleared once the match is verified, preventing unauthorized access should the computer be tampered with or damaged. TSA secures passenger PII against risk of loss, unauthorized access, or use through a variety of information technology safeguards.

Privacy Risk: There is a privacy risk of unauthorized access to the checkpoint hardware and related data transmissions.

Mitigation: This risk is mitigated. TSA employs mandatory federal data encryption standards (in accordance with Federal Information Processing Standard (FIPS) 140-3 and 197 as applicable) for all data at rest and in transit. Additionally, the system requires multi-factor authentication by authorized users via a TSA-issued PIV card and PIN to login to the system for screening activities. The system also makes use of auto-logoff capabilities.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TSA personnel operating the Secure Flight and CBP TVS programs are given training in systems operation protocols. Additionally, personnel receive training on how to protect passenger privacy.

TSA personnel are assigned roles for accessing the system based on their function. The system administrator grants access to authorized users based on the principles of need-to-know, least privilege, and separation of duties. The Information System Security Officer (ISSO) confirms policy compliance and manages the activation or deactivation of accounts and privileges as required or when expired.

System user access for Secure Flight and CBP TVS can be analyzed and audited by the system owner and ISSO to ensure that data and reports are accessed only by individuals with a need-to-know and for authorized purposes.

All TSA and contractor personnel are required to comply with DHS/TSA privacy policies. Access controls are currently in place (including technological controls) to ensure only authorized personnel may access the information. The program manager of the proof of concept may audit the examination, maintenance, destruction, and usage activities to ensure they are used as described and that privacy and security protections are followed.

Conclusion

As part of its on-going efforts to enhance the identity verification of passengers by using facial identification technology at airport, TSA is expanding upon its previous facial identification proofs of concept. TSA is continuing to leverage CBP's TVS to pre-stage a gallery of passenger photo templates for certain TSA PreCheck® passengers who opt-in to using their photograph for identity verification at the checkpoint. As explained above, these efforts will expand to other airports and airlines beyond those identified in the previous PIA.

Contact Official

Jason Lim
Identity Management Capability Manager
Transportation Security Administration
Jason.Lim@tsa.dhs.gov

Responsible Official

Peter Pietra
Privacy Officer
Transportation Security Administration
TSAprivacy@tsa.dhs.gov

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717