Privacy Impact Assessment

for the

Travel Document Checker Automation Using Facial Identification

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

January 28, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Transportation Security Administration (TSA) will enhance the identity verification of passengers by using facial identification[1] technology at airports. In previous proofs of concept, TSA used a Credential Authentication Technology (CAT) device equipped with a camera to validate that the identity document presented by the passenger was authentic and to compare the passenger's live facial image against the image from the passenger's identity document. TSA will conduct a new proof of concept to be held at Detroit Metropolitan Wayne County Airport in cooperation with Delta Airlines. In the new proof of concept, TSA will test using the U.S. Customs and Border Protection (CBP) Traveler Verification Service (TVS) to pre-stage a gallery of passenger photographs for certain TSA PreCheck™ and CBP Global Entry passengers who **opt-in** during the check-in process to have their image captured and use their photograph(s) already on file with DHS for identity verification at TSA checkpoints. Only CBP Global Entry passengers and TSA PreCheck™ passengers who have a U.S. passport will be eligible to participate in this proof of concept. Data from the proof of concept will be shared with the DHS Science and Technology Directorate (S&T) for subsequent qualitative and quantitative analysis.[2]

This Privacy Impact Assessment (PIA) is conducted pursuant to Section 222 of the Homeland Security Act to address privacy risks in the use of technology to connect the CBP TVS to the TSA checkpoint identity verification systems to allow for the potential of allowing passengers to transit the TSA checkpoint.

Introduction

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 area of airports.[3] As part of its efforts to secure aviation transportation, TSA verifies passenger identities before granting access to airport sterile areas. The TSA Transportation Security Officer (TSO) performing Travel Document Checker (TDC) functions currently verifies identity at the checkpoint by validating the identity document and boarding pass presented by the

[1] The National Institute of Standards and Technology (NIST) uses "facial identification" as a "1 to many" search used to determine whether an individual in a photo is a match to any photos in a database. "Facial verification" or "1:1" matching confirms a photo matches a different photo of the same individual in a database or the photo on a credential. Both are types of facial recognition technology. *See* https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0.

[2] In accordance with 5 U.S.C. § 552a(b)(1) and DHS/TSA-001 Transportation Security Enforcement Record System (TSERS), 83 Fed. Reg. 43888 (August 28, 2018), Routine Use A, *available at* https://www.dhs.gov/system-records-notices-sorns.

[3] "Sterile areas" are portions of airports that provide passengers access to boarding aircraft and to which the access generally, is controlled by TSA, or by an aircraft operator or a foreign air carrier through the screening of persons and property (49 CFR Part 1540.5).

passenger, visually comparing the photograph on a passenger's identity document to the passenger's face, and then comparing the document's biographic information to the biographic information on the passenger's boarding pass.[4] Once those steps are successfully completed, the passenger proceeds to security screening.

To improve the security, speed, and efficiency of TSA's checkpoint identity verification process, TSA is exploring the use of biometric matching technologies,[5] with a focus on facial identification as the primary means of identity verification for aviation security screening. TSA expects that using facial identification may permit TSA to improve airport security and expedite checkpoint security processes.

In previous proofs of concept, TSA demonstrated the ability to use CAT devices with a camera (CAT-C) and connections through TSA's Security Technology Infrastructure Program (STIP)[6] to the TSA Secure Flight system[7] in order to perform the biometric match at the CAT-C device, match the passenger's identity from the identity document directly against the information provided in the Secure Flight system, and obtain the appropriate boarding pass instruction. TSA transmitted a subset of Secure Flight Passenger Data (SFPD) for passengers traveling that day at that airport to CAT-C devices at security checkpoints via TSA's STIP data management system. SFPD transmitted to the CAT-C included:

- 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; and
- Record sequencing/versioning information.

[4] For passengers who are unable to present verifying identity documentation, TSA offers an alternative identity verification process in which passengers answer knowledge-based questions.
[5] DHS defines biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition." *See* https://www.dhs.gov/biometrics.
[6] STIP is a suite of TSA applications that provide equipment connectivity, data collection, and data reporting.
[7] *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.

The previous proofs of concept relied on a 1:1[8] match of identity against an authenticated identity document that is presented to the TDC. While TSA continues to develop these identity verification concepts, it is also concurrently working on a concept of operation that uses a 1:n[9] match that may permit passengers to travel without presenting an identity document to the TDC. To that end, TSA will partner with CBP to use the CBP TVS[10] system to pre-stage a gallery of passenger photographs for certain TSA PreCheck™ or CBP Global Entry passengers who opt-in (during the check-in process) to use their photograph for identity verification at TSA checkpoints. Only TSA PreCheck™ passengers who have a U.S. passport and CBP Global Entry passengers will be eligible to participate in this proof of concept. Additionally, in order to create a photograph gallery within CBP TVS, TSA PreCheck™ passengers with a U.S. passport and CBP Global Entry passengers desiring to participate must also provide their passport number so that CBP TVS can pull their photograph from existing DHS holdings.[11]

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

Process for this Proof of Concept

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 (Delta) 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 a new technical infrastructure from Secure Flight to CBP TVS to coordinate the CBP TVS query of DHS holdings, stage their templates[12] 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'

[8] 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.
[9] 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.
[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.See DHS/CBP/PIA-056 Traveler Verification System *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-january2020_0.pdf
[11] These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters.
[12] These "templates" are strings of multiple numbers that represent specified images and facilitate facial recognition matching within the secure CBP TVS environment. These templates cannot be reverse engineered for viewing by external parties (meaning if an unauthorized user were to view the template, it would not be visible as a facial image).

boarding passes to ensure that only consenting travelers will enter the queue for the proof of concept.

For purposes of this proof of concept, TSA will require passengers to scan an identity document at the checkpoint, although this concept is designed to be operational without the need for an identity document. 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[13] to CBP TVS. Once the photograph is received in CBP 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 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, quality scores) and outcomes of each transaction (match or no match) for analysis.

Data Retention

CBP TVS

CBP TVS will be used by TSA during this proof of concept for passengers on both international and domestic flights. CBP TVS is the backend matching service for all CBP biometric entry and exit operations that use facial recognition, regardless of travel mode (air, land, or sea). The CBP TVS system conducts backend biometric matching and provides a result to different CBP systems depending on the environment. For all biometric matching deployments, CBP TVS relies on biometric templates generated from pre-existing photographs that CBP maintains, known as a gallery. These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters.

[13] Unique identifier is used to distinguish a record within the list of results returned from CBP TVS. It is a TSA-generated value associated with the transaction (not the individual), concatenated, and made up of departure airport code, departure date time, and Secure Flight vetting instance.

CBP purges all photos, regardless of immigration or citizenship status, from the TVS cloud matching service within 12 hours.[14] CBP is providing its TVS cloud matching service as a service to TSA and makes no further use of the data. TSA has the ability to accept and use the service pursuant to laws[15] that permit TSA to voluntarily accept use or accept the services, equipment, personnel, and facilities of any other federal agency.

TSA

The camera device will delete all transactional metadata and biographic information taken from the identity document when the operator acknowledges the results or starts the next passenger transaction. TSA will delete from the technical infrastructure communicating with CBP TVS the name, gender, date of birth, flight information, vetting status, SFPD, biometric match/no-match response, matching unique identifiers, passport number, passport country, passport expiration date, and passenger photographs captured using the camera device within 24 hours after a passenger's scheduled departure.

Personally identifiable information (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 the retention policy for Secure Flight.

S&T

Data collected during this proof of concept will be shared with S&T for subsequent qualitative and quantitative analysis. S&T will extract biometric images for the purpose of generating biometric templates. This data transformation is not reversible; original biometric images cannot be recovered from the templates. S&T will use the data and information it receives during this pilot solely for the purpose of analysis, and according to the Test Plan developed for the effort. S&T will not use the data provided by TSA for any other purpose, including operational uses within DHS. S&T will consult with NIST during the assessment of the facial-matching algorithm and to assure the analysis methodologies meet industry standards.

S&T will delete the data no later than 180 days following receipt in accordance with an approved TSA record retention schedule for security technology (N1-560-04-14, Item 2).

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[16] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the

[14] *See supra* note 9.
[15] 49 U.S.C. §§ 106(l), (m).
[16] 5 U.S.C. § 552a.

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.[17]

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.[18] 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[19] and the Homeland Security Act of 2002, Section 222.[20] 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 subsequent photograph capture. During check-in, passengers will opt-in and consent to providing PII to pre-stage their photograph and confirm that they have read a Privacy Notice. TSA will provide signage for those passengers who have consented during check-in, in close proximity to the queue at the airport, to provide notice to passengers that permitting TSA to take their photograph is optional and that they can decide not to proceed with participation in the pilot by not consenting to have their photograph taken. 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 their photograph taken. If a passenger declines the live photograph capture, he or she will be directed to standard security screening and 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.

---

[17] 6 U.S.C. § 142(a)(2).
[18] 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.
[19] 44 U.S.C. § 3501 note.
[20] 6 U.S.C. § 142.

Privacy Risk: There is a risk that passengers will not know their photographs are being captured by TSA for identity verification.

Mitigation: This risk is mitigated. The check-in process requires affirmative action including providing a passport number, and the process of taking the photograph is completely overt since it requires the passenger's cooperation to pose for the photo in front of the camera. Consenting passengers may, at any time before their photo is captured, decline the photo capture and request standard security screening and processing. Signs posted in close proximity to the TDC will provide instructions for participating and will inform passengers that taking the photograph is optional and of their ability to seek alternative procedures if they do not wish to participate in the proof of concept. In addition, this PIA and public communications materials will inform members of the public of the procedures for participating.

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 will have the opportunity to read about the proof of concept when they check-in on the airline's mobile application. In addition, this PIA provides information regarding the role of each agency in this proof of concept. Information about the proof of concept will also be available on TSA.gov.

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 the individual to repeatedly 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 their photograph being captured. Individuals will present their identity document to the TDC to be scanned and will follow directions from the TDC for photo capture. If a passenger declines the live photograph capture, he or she will be directed to standard security screening and 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 has the additional purpose of assessing critical 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 for securing aviation transportation and specifically authorizes TSA to test new technology and equipment.[21] 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.[22] TSA has 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.[23] The agency also has authority to strengthen access control points by deploying biometric or similar technologies to ensure security of passengers and aircraft.[24] Under ATSA, TSA is responsible for, among other things, security in all modes of transportation;[25] screening operations for passenger air transportation;[26] receiving, assessing, and distributing intelligence information related to transportation security;[27] assessing threats to transportation;[28] coordinating countermeasures;[29] and carrying out such other duties relating to transportation security as it considers appropriate.[30] Finally, the TSA Modernization Act requires a report that includes from TSA, as well as CBP, specific assessments regarding the impacts of the use of biometric technology.[31]

4. Principle of Data Minimization

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 will collect only the PII directly relevant and necessary to perform identity verification, and to assess critical operational and technological components of the biometric matching. TSA will

[21] 49 U.S.C. § 114(f)(8), (9).
[22] Pub. L. 107-71, § 109(a)(7) (November 19, 2001) (codified at 49 U.S.C. § 114 note).
[23] 49 U.S.C. § 44903(c)(2)(3).
[24] 49 U.S.C. § 44903(g)(2)(G).
[25] 49 U.S.C. § 114(d).
[26] 49 U.S.C. § 114(e).
[27] 49 U.S.C. § 114(f)(1).
[28] 49 U.S.C. § 114(f)(2).
[29] 49 U.S.C. § 114(f)(4).
[30] 49 U.S.C. § 114(f)(15).
[31] TSA Modernization Act, Pub. L. 115-254, § 1919(c) (October 5, 2018).

collect:

- 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); and
- Outcomes of each transaction (match or no match) only from passengers who volunteer to participate.

Only passport information, KTN, live photo, name, gender, date of birth, and departure airport/time will be passed to CBP TVS.

TSA will minimize the collection of PII by limiting the amount of Secure Flight data passed to the checkpoint. Only the local Secure Flight data for a specific airport will be passed to the checkpoint at the airport involved with this proof of concept.

Data collected during the proof of concept will also be transferred to S&T for analysis. Specifically, TSA will collect, encrypt, and transmit to S&T:

- Name;
- DOB;
- Gender;
- Identification type/state of issuance; and
- 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.

S&T will delete the data no later than 180 days following receipt in accordance with an approved TSA record retention schedule for security technology (N1-560-04-14, Item 2). S&T will evaluate the performance of the camera system (e.g., failure to acquire rate) and evaluate system matching performance (e.g., false match rate, false non-match rate). The results of the evaluation will be used to help inform future TSA plans and biometrics requirements development and identify and mitigate any performance issues and operational concerns.

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

Mitigation: This risk is mitigated. The camera device will delete all transactional metadata and biographic information taken from the passenger's identity document when the TDC operator acknowledges the results or starts the next passenger transaction. TSA will purge 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); and
- 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 will maintain the data for no more than 180 days after receipt at which time it will be deleted in accordance with TSA's applicable record 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 match a live photograph against the gallery, and with 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.[32]

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 will only use the biometric data to perform identity verification at the checkpoint, and to assess critical operational and technological components of the pilot. CBP TVS is only used for identity verification. Because this proof of concept is only available to passengers who are enrolled in the TSA PreCheck™ who have a U.S. passport and CBP Global Entry programs, passenger information that is shared with CBP for purposes of the proof of concept does not create the risk of 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 his or her identity in accordance with standard TSA procedures.

Privacy Risk: There is a risk that the facial images collected through and compared in TVS, will not be of high enough quality or not be an accurate representation of the traveler, negatively impacting the reliability of the matching service.

Mitigation: This risk is mitigated. CBP and TSA are continually testing and evaluating 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 ensure there are no adverse impacts. CBP and TSA are also partnering with S&T to evaluate algorithms and test biometric technologies developed by specified vendors.

[32] *See* DHS/TSA-019 Secure Flight Records, 80 Fed. Reg. 233 (January 5, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

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.

Authorized users of the checkpoint hardware used in this proof of concept will be limited to the TSA personnel staffing the device. The hardware will be physically locked when not in use, and there will be access control on the government-furnished computer including login with an active Personal Identity Verification (PIV) card. 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 and unauthorized access or use through a variety of information technology safeguards.

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

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 in transit and at rest. Additionally, the system requires authorized users to log in to the system with a TSA-issued PIV card to log in to the system for screening activities. The system also uses 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 appropriate systems 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, including annual privacy training required by DHS. 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 airports, TSA will leverage CBP TVS to pre-stage a gallery of passenger photographs for certain TSA PreCheck™ and CBP Global Entry passengers who opt-in to use their photograph for identity verification at TSA checkpoints. TSA will continue to work with its CBP and S&T partners, as well as the DHS Privacy Office, to ensure adequate privacy measures are taken.

Contact Official

Jason Lim
Identity Management Capability Manager TSA Biometrics
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 copy on file at the DHS Privacy Office.

_____

James Holzer
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717