Privacy Impact Assessment for
the

Travel Document Checker Automation Using Facial Verification

DHS/TSA/PIA-046(b)

June 03, 2020

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

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Transportation Security Administration (TSA) will enhance the identity verification of passengers by using facial verification technology at airports. In a previous proof of concept, TSA used a Credential Authentication Technology (CAT) device equipped with a camera (CAT-C) 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. Building on its previous work, TSA will now network the CAT-C to the TSA Secure Flight system so that passenger boarding pass information can be passed from Secure Flight to the CAT-C. This will provide improved real-time boarding pass instructions with improved identity matching and reduced physical handling of travel documents to limit unnecessary exposure, such as during the Coronavirus (COVID-19) pandemic.

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 in connecting the CAT-C to the TSA Secure Flight system, displaying Secure Flight data on the CAT-C, and integrating Secure Flight data in the identity verification process.

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.[1] 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 manually validating the identity document and boarding pass presented by the passenger, 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 passenger's boarding pass.[2] Once those steps are successfully completed, the passenger proceeds to security screening. The next section will explain how TSA intends to modify this process using facial verification.[3]

[1] "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).
[2] For passengers who are unable to present verifying identity documentation, TSA offers an alternative identity verification process in which passengers answer knowledge-based questions.
[3] TSA is realigning terminology to follow the National Institute of Standards and Technology's (NIST) usage of "verification" (1:1 matching).

Facial Verification

To improve the security, speed, and efficiency of TSA's checkpoint identity verification process, TSA is exploring the use of biometric matching technologies,[4] with a focus on facial verification "as the primary means of identity verification for aviation security screening."[5] TSA expects that facial verification may permit TSA personnel to improve security by focusing on other critical tasks and expedite checkpoint security processes.

In a previous proof of concept, TSA used a CAT device equipped with a camera at the checkpoint.[6] The CAT-C validated that the identity document presented by the passenger was authentic; collected the photo image and biographic information of the passenger from the document; and captured the passenger's live facial image. The CAT-C device compared the facial image of the individual taken at the checkpoint to the image from the passenger's identity document using a proprietary facial matching algorithm to verify that the document belonged to the person presenting it.

Building on this prior proof of concept, TSA expects to connect the CAT-C device through TSA's Security Technology Infrastructure Program (STIP)[7] to the TSA Secure Flight system[8] 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 will transmit 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 includes passengers' full name, gender, date of birth, as self-reported when the reservation was made, plus passport information (if available), itinerary information (flight number, departure/arrival airports and times), known traveler number (if available), passenger record locator, reservation status, assigned boarding pass printing result, and record sequencing/versioning information.

Process

TSA will test and may implement a physical configuration for the CAT-C that enables the passengers to self-scan their own identity documents in the appropriate scanners (one for driver's licenses and similar-sized cards and another for passports) without handing the identity documents to the TSOs performing the TDC functions. This configuration was developed specifically to minimize

[4] DHS defines biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition." *See* https://www.dhs.gov/biometrics.
[5] *See* TSA Biometrics Roadmap For Aviation Security & the Passenger Experience (September 2018), *available at* https://www.tsa.gov.
[6] *See* DHS/TSA/PIA-024 Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS), *available at* https://www.dhs.gov/privacy.
[7] STIP is a suite of applications that provide equipment connectivity, data collection, and data reporting.
[8] *See* DHS/TSA/PIA-018 Secure Flight, *available at* https://www.dhs.gov/privacy.

physical interaction between passengers and the TSOs at the TDC station and eliminate to the extent possible the need to exchange the identity documents. Rather than passengers handing over the identity documents to the TSOs to insert into the scanners, passengers will approach the CAT-C device insert their own identity documents into the scanner appropriate to their chosen identity document type.

The CAT-C scan will authenticate the identity document and temporarily capture certain biographic information from the identity document, which includes name, gender, and date of birth (as printed on the identity document); image of the front and back of the identity document; and other non-PII information such as document type (e.g., driver license, passport). The name, gender, date of birth, and non-PII information will be compared within STIP to information provided by Secure Flight against the self-reported data input by the passenger at the time of reservation. The CAT-C device will then display the passenger's results for TDC review of face matching, ID authentication, and Secure Flight information on the CAT-C. It will also display the image of the passenger obtained at the checkpoint and the passenger's photo from the ID. Finally, the TDC officer will conduct any resolution procedures if necessary and direct passengers to the appropriate screening lane. This process allows the TDC to cross-check the biographic information from the passenger's identity document directly against the passenger's SFPD to ensure that the data is the same, verifying the passenger should be at that airport that day and ensuring the passenger receives the appropriate level of screening.

Passengers may decline to have a photo taken at the checkpoint but will still be required to place their identity document in the CAT-C for verification against SFPD. If a passenger opts out of the photo, the CAT-C device will not take the photo but will still read the passenger's identity document and compare it to SFPD. Signs will be posted providing travelers with notice of the CAT-C, along with the option to opt-out of the CAT-C taking their photo.

Retention in Routine Operations

The data associated with the CAT-C falls into two groups: 1) data already held by TSA in the Secure Flight system that is sent to the CAT-C through STIP, and 2) data that is captured by the CAT-C when the passenger presents an ID and has a photo taken. In the course of regular screening operations, TSA will delete the Secure Flight data stored on CAT-C within 24 hours of the original flight departure time. As to the data captured by the CAT-C, each passenger's PII collected from the identity document and photo will be overwritten when the next scan occurs, and when the TDC officer logs off the CAT-C device.[9]

Retention for Test Purposes

Because TSA expects to deploy the CAT-C in a rapid manner, it will have a need to continue to evaluate system performance as well as test new algorithms and software changes in an operational

[9] As an additional safeguard, the CAT-C is configured to automatically log-off if there has been 30 minutes of inactivity, which will delete the last passenger's PII.

setting. TSA will conduct testing on its own as well as with DHS Science & Technology (S&T). Data will be collected by TSA and retained for subsequent qualitative and quantitative analysis by TSA and S&T. The test data will be obfuscated to the greatest extent possible and will be stored on a removable TSA-owned encrypted hard drive attached to the CAT-C. TSA personnel will remove the encrypted hard drive and securely transfer it to S&T personnel. Exchanging the hard drives will help to minimize any potential corrupted data and will allow S&T to start qualitative and quantitative analysis before testing concludes.[10] In order to support system improvements, TSA may from time to time configure a small number of CAT-C devices for a short period of time to retain passenger data from the ID and photo for up to 24 months in order to evaluate system performance. Signs will be posted providing travelers with notice of the temporary data collection event at CAT-C and proposed retention period, along with the option to choose a manual checkpoint process as an alternative.

The passenger data that will be collected for this type of analysis is as follows: real-time images of the passenger's face (live photo from the checkpoint); passenger's photograph from the identity document; identification document issuance and expiration dates; date of travel; the type of identification document; the organization that issued the identification document (e.g., the state that issued the passenger's driver's license, or the U.S. Department of State in the case of passports); year of passenger's birth; gender as listed in the identification document; obfuscated identification document number; obfuscated passenger name as listed in the document; and obfuscated date of birth as listed in the document. The CAT-C will "obfuscate" typewritten PII scanned from the face page of the identification document presented. This limited PII will be replaced with a code that cannot be used to recreate the PII, but still allows confirmation that the credential is unique.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[11] 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.[12]

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.[13] The FIPPs account for the

[10] *See* DHS/TSA/PIA-046(a) Travel Document Checker Automation Using Facial Recognition, *available at* https://www.dhs.gov/privacy.
[11] 5 U.S.C. § 552a.
[12] 6 U.S.C. § 142(a)(2).
[13] *See* 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," *available at*

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[14] and the Homeland Security Act of 2002 Section 222. [15] This PIA examines the privacy impact of the use of biometric technology as part of this new proof of concept in relation 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 personally identifiable information (PII). Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

TSA will provide signage in close proximity to the queue at the airport to provide notice to passengers. Signs will provide travelers information regarding the procedures for participating, as well as instruction on not having their photo taken if they choose not to participate. If a passenger chooses not to participate, the signage will advise the passenger that his or her identity document will still be scanned to verify their identity. 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 their photographs are being captured by TSA for identity verification.

Mitigation: This risk is mitigated. The process for taking the photograph is completely overt and obvious since it requires the passenger's cooperation to pose for the photo in front of the camera. In addition, this PIA, along with signs posted in close proximity to the CAT-C and public communications materials, will inform members of the public of the procedures for participating and that TSA will take their photo and attempt to match the facial image with the biometric image from their identity document. Signage and public communications materials will also inform members of the public of their ability to seek manual procedures if they do not wish to participate in the 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

https://www.dhs.gov/privacy.
[14] 44 U.S.C. § 3501.
[15] 6 U.S.C. § 142.

redress regarding DHS's use of PII.

Signs in close proximity to the queue will provide notice to passengers about how to participate. Individuals will present their identity document to the CAT-C device to be scanned and to initiate photo capture. The CAT-C device will display results for face matching, ID authentication, and Secure Flight information to the TDC officer. The TDC officer will direct passengers to the appropriate screening lane and conduct any resolution procedures as necessary. All passengers proceeding through the dedicated queue will have the option to decline having their photo taken and can request manual identity verification by a TDC officer.

Through the Secure Flight program, TSA collects certain information from U.S. aircraft operators and foreign air carriers to identify and prevent known or suspected terrorists from boarding aircraft or accessing sterile areas. SFPD consists of name, gender, date of birth, passport information (if available), itinerary information (flight number, departure/arrival airports and times), known traveler number (if available), passenger record locator, reservation status, assigned boarding pass printing result, and record sequencing/versioning information. Secure Flight information is used to issue an appropriate boarding pass instruction for screening.

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 CAT-C permits TSA to verify the content of the identity document and/or boarding pass against the data contained in Secure Flight that generated the boarding pass instruction.

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, and assess critical operational and technological components of the CAT-C. 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.[16] 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.[17] 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.[18] The agency also has authority to strengthen access control points by deploying biometric or similar technologies to ensure

[16] 49 U.S.C. § 114(f)(8), (9).
[17] Pub. L. 107-71, § 109(a)(7) (November 19, 2001) (codified at 49 U.S.C. § 114 note).
[18] 49 U.S.C. § 44903(c)(2)(3).

security of passengers and aircraft.[19] Under ATSA, TSA is responsible for, among other things, security in all modes of transportation;[20] screening operations for passenger air transportation;[21] receiving, assessing, and distributing intelligence information related at transportation security;[22] assessing threats to transportation;[23] coordinating countermeasures;[24] and carrying out such other duties relating to transportation security as it considers appropriate.[25] Finally, the TSA Modernization Act required a report that includes from TSA, as well as U.S. Customs and Border Patrol (CBP), specific assessments regarding the impacts of the use of biometric technology.[26]

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 CAT-C. TSA will only collect facial images and biographic information from passengers who volunteer to participate.

TSA will minimize the collection of PII by limiting the amount of Secure Flight data passed to the CAT-C devices. Only the local Secure Flight data for a specific airport will be passed to the CAT-C devices at that airport. TSA will further minimize the amount of information stored in STIP by transmitting only a subset of Secure Flight information, specifically passenger's name, gender, and date of birth, as self-reported by the passenger when making his or her reservation, plus Secure Flight screening status, reservation control number, and flight itinerary[27] from the Secure Flight to STIP.[28] STIP will then send the data, received from Secure Flight, to the CAT-C device. Consistent with current CAT procedures,[29] only the Secure Flight data for passengers scheduled to fly from a specific airport will be sent to CAT-C devices at that airport. The name, gender, date of birth, and

[19] 49 U.S.C. § 44903(g)(2)(G).
[20] 49 U.S.C. § 114(d).
[21] 49 U.S.C. § 114(e).
[22] 49 U.S.C. § 114(f)(1).
[23] 49 U.S.C. § 114(f)(2).
[24] 49 U.S.C. § 114(f)(4).
[25] 49 U.S.C. § 114(f)(15).
[26] TSA Modernization Act, Pub. L. 115-254, § 1919(c) (October 5, 2018).
[27] Flight itinerary data will be used to assist STIP in distributing information destined for CAT/BPSS devices to the correct airport.
[28] Secure Flight data used for CAT/BPSS purposes do not include passport information, redress, Known Traveler number, record sequence number, record type, passenger update indicator, and traveler reference number. More information on the Secure Flight program may be found in previously published PIAs located at: http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.
[29] *See* DHS/TSA/PIA-024(b) Credential Authentication Technology/Boarding Pass Scanning System (January 18, 2013), *available at* https://www.dhs.gov/privacy.

non-PII information will be sent back, through STIP, to Secure Flight to compare against the self-reported data provided by the passenger.

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

Mitigation: This risk is mitigated. In accordance with current CAT procedures,[30] PII from Secure Flight will be retained 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. Images will be retained until the next transaction is processed or when the TSO logs off the system. System auto logoff is set at 30 minutes of inactivity. PII sent back to Secure Flight will follow Secure Flight's retention policy.

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.

Information garnered from the CAT-C will be used for the purpose specified in the notice: to verify identity, test the CAT-C functionality, determine its ability to compare accurately a passenger's facial image on his or her identity documents with the passenger's photo taken at the checkpoint, and incorporate passenger Secure Flight information. The data generated on CAT-C devices is not used for any purpose other than as discussed in this PIA or the previous PIAs where CAT devices with Secure Flight connectivity are deployed.

PII temporarily stored on CAT-C will not be shared outside of TSA. 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.[31]

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 obtained from Secure Flight for CAT-C purposes is the same information that individuals present to a TSO during the ID verification process. When the CAT-C scans an identity document, TSA obtains the passenger's name, gender, and date of birth from the identity document. An image of the ID is captured to present to the TSO. The comparison of information between Secure Flight and CAT-C via STIP provides TSA greater assurance that passenger identity documents are not

[30] *See* DHS/TSA/PIA-024(b) Credential Authentication Technology/Boarding Pass Scanning System (January 18, 2013), *available at* https://www.dhs.gov/privacy.
[31] DHS/TSA-019 Secure Flight Records, 80 FR 233 (January 5, 2015).

fraudulent and have not been altered. The comparison ensures data accuracy by providing near real-time updates from Secure Flight to the CAT-C devices, which enhances transportation security.

If name mismatches occur, CAT-C will display a list of Secure Flight data on passengers with similar attributes (e.g., the same date of birth, gender, last name, and/or first name) that are scheduled to travel on the same day at the assigned airport in order to compare data and resolve name mismatches. In the event that the comparison identifies a fraudulent document, TSA will investigate and may retain information on the incident within the Performance and Results Information System (PARIS).[32] CAT-C prohibits name-based searches or retrieving additional PII. TSA does not store or maintain any additional PII displayed on the screen of the CAT-C unit.

Privacy Risk: There is a risk that inaccurate information could be sent to the CAT-C devices.

Mitigation: This risk is mitigated. TSA obtains the information directly from a trusted TSA data source and by using secure data transmission techniques described further in Section 7, Principle of Security. Additionally, if any issues arise during the process, the TDC officer will conduct resolution procedures as necessary.

Privacy Risk: There is a risk that TSA's cameras will be unable to capture images of a high enough quality to produce accurate matches, resulting in TSA's inability to confirm traveler identities.

Mitigation: This risk is mitigated. If CAT-C is unable to match a passenger's photo, or experiences any error during the process, the passenger will be screened according to the normal manual TDC process.

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 CAT-C will be limited to the TSA personnel staffing the device. Close accountability of the CAT-C and the removable drives will be maintained at all times. The CAT-C will be physically locked when not in use, and there will be access control on the CAT-C computer including login with an active Personal Identity Verification (PIV) card. In the unlikely event the CAT-C is tampered with or damaged, it is programmed to automatically delete all of its data. TSA secures passenger PII against risk of loss and unauthorized access or use through a variety of information technology safeguards.

[32] *See* DHS/TSA/PIA-038 Transportation Security Administration Performance and Results Information System (PARIS), *available at* https://www.dhs.gov/privacy.

Privacy Risk: There is a privacy risk of exposing the CAT-C unit 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 CAT-C 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.

Privacy Risk: There is a risk that employees without a need-to-know the information in the performance of official duties may receive access to Secure Flight data.

Mitigation: This risk is mitigated. The CAT-C device will only display biometric matching results, ID authentication results, and Secure Flight information to the TSO operating the device or supervisors summoned to resolve passenger identity document and/or boarding pass validation matters. Additionally, TSA will adhere to Secure Flight security safeguards outlined in previously published PIAs, which include administrative and technical controls to protect information against unauthorized disclosure, use, modification, or destruction.

Privacy Risk: There is a risk that passenger PII on display monitors will be visible to other passengers.

Mitigation: This risk is mitigated. TSA positions CAT-C monitors away from passengers and employs privacy screens that help prevent individuals from viewing the information.

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, STIP, and CAT-C 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, STIP, and CAT-C 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 CAT-C. 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

Building on its previous work, TSA will network the CAT-C to the TSA Secure Flight system so that passenger boarding pass information can be passed from Secure Flight to the CAT-C. This will provide improved real-time boarding pass instructions with improved identity matching and reduced physical handling of travel documents with reduced risk of exposure to Coronavirus (COVID-19).

Responsible Officials

Jason Lim
Identity Management Capability Manager TSA Biometrics
Transportation Security Administration
Department of Homeland Security

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security