Privacy Impact Assessment Update
for

Credential Authentication Technology/ Boarding Pass Scanning System

DHS/TSA/PIA-024(b)

January 18, 2013

Contact Point
James M. Johnson
Program Manager, Office of Security Capabilities
Transportation Security Administration
James.M.Johnson1@tsa.dhs.gov

Reviewing Official

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) validates the authenticity of passenger identity documents and/or boarding passes at Transportation Security Administration (TSA) security checkpoints. TSA is updating its Privacy Impact Assessment (PIA) to reflect that it will network CAT/BPSS in order to transmit data from the Secure Flight[1] database to CAT/BPSS devices at security checkpoints. This PIA update applies to all locations where TSA will pilot and deploy Secure Flight connectivity. Where TSA continues to operate CAT/BPSS devices without Secure Flight connectivity, the previously published PIAs dated November 29, 2007 and August 11, 2009,[2] remain in effect. This activity does not alter the privacy posture of the data obtained previously by TSA for the Secure Flight program.

Introduction

TSA has deployed means for validating passenger identity documents and/or boarding passes. Notwithstanding these efforts, certain security vulnerabilities associated with boarding passes remain. In response to these vulnerabilities, TSA previously integrated its Credential Authentication Technology (CAT) with its Boarding Pass Scanning System (BPSS) technology. The goal of CAT/BPSS is to ensure that identity documents and/or boarding passes presented at the checkpoint have not been tampered with or fraudulently produced. Using CAT/BPSS, TSA verifies the authenticity of a passenger identity document by comparing its format and security features against a known set of security features for that particular identity document type. While TSA previously operated each CAT/BPSS device as a stand-alone system that provided no network connectivity or data retention capabilities, the CAT/BPSS now displays machine readable data from the identity document and/or boarding pass for visual confirmation against the human readable portions of those documents to verify that the documents are authentic and, after visual identification by the Travel Document Checker (TDC), belong to the individual presenting the documents. Validation of the document's security features provides TSA greater assurance that the passenger identity document was not fraudulently produced and has not been altered.

In its efforts to address the security vulnerabilities in the authentication of passenger identity documents and/or boarding passes, TSA will send certain Secure Flight data to generate the boarding pass outside of the airport security area; then through TSA's Security Technology

[1] 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.
[2] DHS/TSA/PIA-024 - Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_catbpss.pdf.

Integrated Program (STIP)[3] to CAT/BPSS inside of the airport security area. This process allows the TDC to verify the content of the identity document and/or boarding pass presented by the passenger directly against the content of the Secure Flight database that generates the boarding pass instruction. TSA will transmit passengers' full name, gender, date of birth, Secure Flight screening status, reservation control number, and flight itinerary[4] from the Secure Flight database to STIP.[5] STIP will then send the Secure Flight data to the CAT/BPSS devices. The data will be securely transmitted in such a way that only the Secure Flight data for passengers scheduled to fly from a specific airport will be sent to CAT/BPSS devices at that airport. If name mismatches occur, CAT/BPSS 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 their assigned airport in order to compare data and resolve name mismatches. TSA will delete the data from STIP and the CAT/BPSS devices within twenty-four (24) hours of the flight departure time. This process will apply to all locations where TSA will pilot and deploy Secure Flight connectivity.

The STIP interface allows the CAT/BPSS device to temporarily maintain a local copy of the passenger's Secure Flight data 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. It is expected in the future to provide the capability to generate non-PII statistical information such as passenger throughput and information on the operating status of the system.

Reason for the PIA Update

TSA is updating its PIA to reflect it will transmit passengers' full name, gender, date of birth, Secure Flight screening status, reservation control number, and flight itinerary from the Secure Flight database to CAT/BPSS devices at security checkpoints via TSA's STIP data management system. TSA will delete the data from STIP and the CAT/BPSS devices within twenty-four (24) hours of the flight departure time.

---

[3] The TSA STIP system assists managers in more effectively administering airport security equipment by providing security patches, software updates, and statistical data to TSA employees and contractors that manage the particular airport security device. It also collects and stores screener performance data, monitors screening equipment status, and collects security equipment throughput and performance data.

[4] Flight itinerary data will be used to assist STIP in distributing information destined for CAT/BPSS devices to the correct airport.

[5] Secure Flight data used for CAT/BPSS purposes does 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

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 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 (PII). 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 and shall assure that technology sustains and does not erode privacy.

In response to this obligation, the DHS Privacy Office has developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act, which encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure. Given the particular technologies and the scope and nature of their use, TSA used the DHS Privacy Office FIPPs PIA template.

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. There should be no system the existence of which is a secret.

TSA previously published PIAs regarding CAT/BPSS on November 29, 2007 and August 11, 2009. This PIA update reflects that TSA will transmit Secure Flight data[6] to CAT/BPSS devices at security checkpoints via STIP and will temporarily store that data (full name, date of birth, gender, Secure Flight screening status, reservation control number, and flight itinerary) in STIP and on CAT/BPSS devices for identity verification purposes. TSA will delete the data in STIP and on the CAT/BPSS devices within twenty-four (24) hours of the flight departure time. This program does not collect new PII or use existing PII (information submitted by passengers during the airline reservation process) for a different purpose. TSA is conducting this PIA to update its efforts to provide transparency and notice to the public regarding TSA's use of CAT/BPSS technologies.

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

[6] This use is consistent with DHS/TSA-019, Secure Flight Records, November 19, 2012, 77 FR 69491. See https://www.federalregister.gov/articles/2012/11/19/2012-28058/privacy-act-of-1974-system-of-records-secure-flight-records.

maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

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/BPSS 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.

TSA will manually resolve anomalies or discrepancies with document validity or identity verification associated with the CAT/BPSS technology at the checkpoint. Individuals may seek access to their records in Secure Flight in accordance with procedures outlined in the Secure Flight PIA;[7] however, information on individuals who are not a match or possible match to a watchlist are deleted within 7 days of the completion of the one-way itinerary, and information in the STIP and/or CAT/BPSS is retained for no more than twenty-four (24) hours from the departure time.

3. Principle of Purpose Specification

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

Pursuant to 49 U.S.C. § 114, TSA is responsible for security in all modes of transportation, including commercial aviation. Under this authority, as well as its general authorities to conduct research and development to enhance transportation security, TSA deployed CAT/BPSS as an improvement over manual inspection of identity documents and/or boarding passes by TSA personnel.

In response to certain well-known security vulnerabilities associated with boarding passes, TSA deployed CAT/BPSS to ensure that identity documents and/or boarding passes presented at the checkpoint have not been tampered with or fraudulently produced. Secure Flight data integration allows TSA to further mitigate these vulnerabilities by confirming the content of the identity document and/or boarding pass presented by the passenger against the content of the Secure Flight database that generates the boarding pass instruction.

4. Principle of 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

[7] A detailed discussion of the Secure Flight program may be found in previously published PIAs - http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight_update018(e).pdf .

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 minimizes the manner in which it uses PII for identity document and boarding pass verification by limiting the amount of Secure Flight data passed to the CAT/BPSS devices. Only the local Secure Flight data for a specific airport will be passed to the CAT/BPSS devices at that airport. TSA further minimizes the amount of information stored in STIP to several specific fields of Secure Flight data: full name, gender, date of birth, Secure Flight screening status, reservation control number, and flight itinerary. TSA does not obtain additional information from passengers for CAT/BPSS operations. Additionally, TSA personnel may only access the information in the system by scanning the identity document and/or boarding pass. The system does not store any PII not already described as 'Secure Flight data' from identity documents; images and other PII are automatically deleted after each transaction. TSA personnel at the CAT/BPSS cannot query Secure Flight for passenger data without the passenger's document and/or boarding pass. TSA will delete the data from STIP and the CAT/BPSS devices within twenty-four (24) hours of the flight departure time.

The privacy risk associated with data retention is retention for longer than is necessary. PII is retained no longer than twenty-four (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.

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.

The CAT/BPSS system is designed to ensure that identity documents and/or boarding passes presented at the checkpoint have not been tampered with or fraudulently produced. The data generated on CAT/BPSS devices is not used for any purpose other than as discussed in this PIA or the previous PIAs[8] where CAT/BPSS devices with Secure Flight connectivity are deployed.

PII temporarily stored on CAT/BPSS 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, November 19, 2012, 77 FR 69491.

[8] DHS/TSA/PIA-024 - Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_catbpss.pdf

6. Principle of Data Quality and Integrity

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

The PII obtained from Secure Flight for CAT/BPSS purposes is the same information that individuals submit during the airline reservation process. TSA does not obtain additional information from passengers for CAT/BPSS operations.

The interface between Secure Flight and CAT/BPSS via STIP provides TSA greater assurance that passenger identity documents and/or boarding passes were not fraudulently produced and have not been altered. The interface ensures data accuracy by providing near real-time updates from Secure Flight to the CAT/BPSS devices, which enhances transportation security.

If name mismatches occur, CAT/BPSS 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 their 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)[9]. CAT/BPSS prohibits name-based searches or retrieving additional PII. TSA does not store or maintain the information displayed on the screen that it used to resolve the mismatch on the CAT/BPSS device or STIP.

The privacy risk associated with data quality and integrity is the possibility that inaccurate information could be sent to the CAT/BPSS devices. TSA mitigates this risk by obtaining the information directly from a trusted TSA data source and by using secure data transmission techniques described further in Section 7, Principle of Security.

7. Principle of Security

Principle: DHS should protect PII, including images, through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The security posture of the CAT/BPSS has changed due to the sharing of PII from the Secure Flight database to the CAT/BPSS devices via the STIP data management system. TSA TDCs will now have visual access to Secure Flight data displayed and stored temporarily on the CAT/BPSS devices.

One of the privacy risks associated with this functionality is the possibility of unauthorized access to data transmissions between the TSA systems. TSA mitigates this risk by

[9] http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_tsa_paris_20120918.pdf

employing mandatory federal data encryption standards (in accordance with Federal Information Processing Standard (FIPS) 140-2 and 197 as applicable) for all data in transit and at rest. Another risk is the possibility that employees without a need-to-know the information in the performance of official duties may receive access to Secure Flight data. TSA mitigates this risk by limiting PII viewing to the TDC operating the display monitor or supervisors summoned to resolve passenger identity document and/or boarding pass validation matters. An additional risk is the possibility that passengers may view PII on the display monitors. TSA mitigates this risk by positioning the monitors away from passengers and employing privacy screens that 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, including images, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

TSA personnel operating within the Secure Flight, STIP, and CAT/BPSS programs are given training in systems operation protocols and processes for protecting the privacy of the traveling public. All TSA personnel are required to take mandatory annual DHS Privacy training.

Additionally, 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/BPSS 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 systems have completed Security Authorization procedures and are Federal Information Security Management Act compliant. Each system has received an Authority to Operate.

9. Additional Issues

Discuss any issues impacting privacy not covered by the eight FIPPs.

None.

Conclusion

Secure Flight data integration into the CAT/BPSS process allows TSA to mitigate security vulnerabilities presented by fraudulent passenger identity documents and/or boarding passes. By using trusted data obtained from Secure Flight via the STIP interface, TSA reduces the reliance on airline data and manual processes to validate passenger identity documents and/or boarding passes. Secure data transmission through a TSA network and deleting the Secure Flight data within twenty-four (24) hours of the flight departure time provides strong privacy protections that do not detract from the security benefits that are to be achieved.

Responsible Officials

James M. Johnson
Office of Security Capabilities
Transportation Security Administration

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security