Privacy Impact Assessment Update
for the

Credential Authentication Technology/ Boarding Pass Scanning System

August 11, 2009

Contact Point
Robin Kane
Assistant Administrator
Operational Process & Technology
robin.kane@dhs.gov

Reviewing Official
Peter Pietra
Director, Privacy Policy & Compliance
Transportation Security Administration
TSAprivacy@dhs.gov

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov

Abstract

The Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) system validates the authenticity of individuals' identity credentials (aka Passenger ID) and boarding passes at the Transportation Security Administration (TSA) security checkpoint and compares the information contained on both documents for consistency. The CAT/BPSS displays machine readable data from an individual's identity credential and boarding pass for confirmation against the human readable portions of those documents to verify that they are legitimate and have not been tampered with. Once confirmed, the displayed data is deleted from the CAT/BPSS.

Reason for this Update

TSA is expanding its document authentication mechanisms to include Credential Authentication Technology (CAT) processes and technologies that validate the authenticity of the identity credential presented at the TSA checkpoint. The integration of CAT with existing BPSS capabilities does not introduce any new privacy risks beyond those previously discussed for BPSS. Unless otherwise noted, the information provided in the November 29, 2007 PIA remains in effect. Individuals are encouraged to read both the November 29, 2007 PIA and this PIA Update to have a complete understanding of TSA's privacy analysis of the CAT/BPSS program.

Introduction

TSA strives to deploy a more efficient and effective means of verifying and validating passengers' travel and identity credentials (passenger ID) to avoid, and when necessary alleviate long lines and potential bottlenecks at transportation facilities. Notwithstanding, certain security vulnerabilities associated with boarding passes are well-known. For example, in fall 2006 a doctoral student at Indiana University created a website that enabled individuals to create fake boarding passes. This website garnered significant media attention, as it demonstrated how a known terrorist on the Watch or No-Fly List could use a fake boarding pass to gain access to the sterile area of the airport. Once inside the sterile area, the terrorist could use a real boarding pass acquired under an alias to board the plane or otherwise disrupt the sterile area.

In response to these vulnerabilities, the TSA is integrating its Credential Authentication Technology (CAT) with its Boarding Pass Scanning System (BPSS) technology. The goal of CAT/BPSS is to ensure that identity credentials and boarding passes presented at the checkpoint have not been tampered with or fraudulently produced. In addition the CAT/BPSS supports TSA efforts to ensure that the information on the boarding pass matches that of the identity credential.

Using CAT/BPSS, TSA verifies the authenticity of the passenger ID by comparing the format and security features of the passenger ID against a known set of security features for that particular identity credential type. Most legitimate forms of identification issued today include some form of encoded data that is written into the credential by the issuing authority in one or more widely accepted formats. The most common formats include one and two dimensional (1D, 2D) barcodes, magnetic stripes, embedded circuits, and machine readable text. The format and security feature set for each credential type are provided to TSA by the credential issuer so that TSA can compare the security features on the passenger ID with the security features provided by the credential issuer. TSA momentarily captures a limited set of

biographic information (Full Name, Date of Birth, and Gender) from the human and machine readable portions of the passenger ID. The system then compares credential data sets to confirm that the human readable data matches the electronically stored data on the passenger ID. The system momentarily captures and displays the photograph from the passenger ID for viewing by TSA to aid in the comparison of the photo to the bearer of the identity credential. Validation of the identity credential's security features and comparison of the credential data sets provides TSA greater assurance that the passenger ID was not fraudulently produced and has not been altered.

CAT/BPSS validates the authenticity of the boarding pass at the TSA security checkpoint using 2D bar code readers and encryption techniques. The system is compatible with any 2D barcode and can be used with paper boarding passes printed on a home computer via online check-in procedures, paper boarding passes printed by the airlines, or a paperless boarding passes that are sent to passengers' mobile devices such as cell phones or Personal Digital Assistants. Authentication of boarding passes can be performed simply with a high degree of security using standard digital signature technology based on Public Key Infrastructure (PKI). When generating the barcode data, the airline creates a hash[1] of the barcode data and then encrypts the hash with the airline's "Private Key." At the checkpoint CAT/BPSS uses the airline's "Public Key" to decrypt the hashed data. The use of a hash function plus encryption allows TSA to confirm that the barcode was issued by the airline and that none of the information in the barcode (such as the passenger's name) has been altered.[2]

CAT/BPSS compares the biographic information captured from the identity credential with the biographic information captured from the boarding pass to determine if the information is identical. This comparison will assist TSA by ensuring that both documents belong to the bearer. TSA does not collect or retain PII any longer than is necessary to confirm that the identity credential and boarding pass are legitimate, have not been tampered with, and are consistent with one another.

The system will alert TSA if either the individual's boarding pass or identity credential does not pass security validation. If the issue is easily rectifiable (e.g., the misspelling of the passenger's name), TSA may resolve the issue immediately and allow the passenger to continue with the security screening process. If the issue cannot be immediately rectified by TSA, the passenger will be directed to the supervisory Transportation Security Officer (TSO) for additional screening.

PII collected by the CAT/BPSS devices is not saved on the device and is immediately deleted after viewing by TSA. Data from previous electronic collections is not retained or displayed.

CAT/BPSS will be deployed initially at airports, but may be used in other transportation environments.

[1] A hash function is a reproducible method of turning some kind of data into a (relatively) small number which identifies the data. The algorithm "chops and mixes" (i.e., substitutes or transposes) the data. The identifiers are called hash sums, hash values, hash codes or simply hashes. Hash sums are commonly used as indices into hash tables or hash files. Cryptographic hash functions are used for various purposes in information security applications.

[2] The hash function creates a unique alphanumeric sequence based on the data in the barcode. Any change in the data results in a change in the alphanumeric sequence generated by the hash.

Fair Information Principles

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information. These concepts are known as the Fair Information Principles (FIPs). The FIPs impose 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.

As such, DHS has developed the Fair Information Principles that underlie the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The DHS Fair Information Principles 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 and the Homeland Security Act of 2002 Section 222. This PIA examines the privacy impact of CAT/BPSS operations as it relates to the Fair Information Principles.

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.

Most PIAs are conducted on IT systems that collect and retain PII. The CAT/BPSS does not use information in this way and, in fact, specifically does not retain any information once the boarding pass has been scanned. TSA is conducting this PIA in order to provide further transparency and notice to the individual regarding the CAT/BPSS. Further, information on the CAT/BPSS is posted to TSA's website.

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.

Consistent with the current screening process, passengers will be aware that their identity credential and boarding pass data will be collected and consent to this collection by proceeding to the checkpoint and providing their documents to TSA. When their information is collected, it is immediately displayed on the device screen in order for TSA to confirm that the identity credential and boarding pass are legitimate and have not been tampered with. The system will alert TSA if either the individual's boarding pass or identity credential does not pass security validation. If the issue is easily rectifiable (e.g., the misspelling of the passenger's name), TSA may resolve the issue immediately and allow the passenger to continue with the security screening process. If the issue cannot be immediately rectified by TSA, the passenger will be directed to the supervisory TSO for additional screening. Once this is completed, the information is permanently deleted from the system.

Fundamentally, the CAT/BPSS merely electronically reads data that should be the same as what a human currently reads off the face of the identity credential and boarding pass.

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.

TSA is responsible for security in all modes of transportation, including commercial aviation under 49 USC §114. Pursuant to that authority, as well as its general authorities to conduct research and development to enhance transportation security, TSA is evaluating the use of the CAT/BPSS as an improvement over current manual inspection of identity credentials and boarding passes by TSA. The PII embedded in the barcode of the boarding pass (including the passenger's name) will be momentarily captured by the CAT/BPSS to compare it to the data generated by the hash function. Additionally a limited set of PII from the electronic portion of the passenger's identity credential will be captured and compared to the PII captured from the boarding pass. If the data matches, the passenger is cleared to proceed.

The information that will be momentarily captured by the CAT/BPPS from the identity credential is limited to Full Name and Date of Birth. Once both the identity credential and boarding pass include Gender CAT/BPPS will also capture Gender. The CAT/BPSS may also momentarily capture and display the photograph to aid the TSA in comparing that picture to the bearer of the identity credential.

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 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).

The CAT/BPSS temporarily displays to TSA limited information contained in the electronic portions of the identity credential and boarding pass. The CAT/BPSS device application does not maintain a transaction log with electronic scan content; the application does not save or store the electronically scanned data to a file, database, etc. This data will be deleted after it is compared. The memory is cleared once the next boarding pass is scanned. Further, when the user exits/closes the CAT/BPSS device application, the form closes and the memory (RAM) storing the scan data is released. When the CAT/BPSS device application is re-launched, the form appears blank and data from previous electronic scans are not available. When the user powers-off the device, any open applications are closed automatically. TSA does not retain any PII any longer than is necessary to confirm that the identity credential and boarding pass are legitimate and have not been tampered with.

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.

None of the PII collected by TSA through the CAT/BPSS will ever be disseminated or shared – not even within the Department. This data will be deleted after it is compared. The memory is cleared once the next boarding pass is scanned.

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 purpose of the CAT/BPSS is to ensure that identity credentials and boarding passes presented at the checkpoint have not been tampered with or fraudulently produced and also supports TSA efforts to ensure that the information on the boarding pass matches that of the identity credential. Validation of the identity credential's security features and comparison of the credential data sets provides the necessary assurance that the passenger ID was not fraudulently produced and has not been tampered with.

The PII collected for CAT/BPSS will be accurate, relevant, timely and complete in terms of airport information.

DHS will utilize a PKI hash function to ensure non-repudiation of the boarding pass data, If the data is incorrect or does not register with the CAT/BPSS device or the PKI hash cannot be validated, TSA will be required to determine if the passenger requires secondary screening.

CAT/BPSS also compares the biographic information captured from the identity credential with the biographic information captured from the boarding pass to determine if the information is identical. This comparison will assist TSA by ensuring that both documents belong to the bearer. The system will alert TSA if either the individual's boarding pass or identity credential does not pass security validation. If the issue is easily rectifiable (e.g., the misspelling of the passenger's name), TSA may resolve the issue immediately and allow the passenger to continue with the security screening process. If the issue cannot be immediately rectified by TSA, the passenger will be directed to the supervisory TSO for additional screening.

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.

All PII collected by the CAT/BPSS devices is not saved on the device and is immediately deleted after viewing by TSA. Data from previous electronic collections is not retained or displayed. These devices employ security safeguards by not maintaining or retaining any PII for longer than needed in order for TSA to perform their job. Additionally, these devices will be protected in accordance with DHS and TSA Security Requirements.

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.

All personnel utilizing the CAT/BPSS devices will receive training. Additionally, the CAT/BPSS will go through normal TSA Certification and Accreditation (C&A) and auditing processes.

9. Other

The system is not configured to store or retain passengers' documents or passengers' PII. The CAT/BPSS is designed to be network compatible for future expansion, however, in its current implementation it is not connected to any network. If TSA determines that networking of CAT/BPSS devices is required TSA will publish an update to this PIA including a discussion of the privacy risks associated with such a change and the mitigation techniques implemented by TSA.

Conclusion

The CAT/BPSS serves to reduce the risk of fraudulent identification credentials or boarding passes. There is a minimal privacy risk to the passenger because of the limited amount of PII momentarily collected from the passenger and because this information is deleted after use. The integration of CAT with existing BPSS capabilities does not introduce any new privacy risks beyond those previously discussed for BPSS in the November 29, 2007 PIA and this PIA Update.

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security