Privacy Impact Assessment
for the

Departure Information Systems Test

DHS/CBP/PIA-030

June 13, 2016

Contact Point
Kim A. Mills
Entry-Exit Transformation Office
Office of Field Operations
U.S. Customs & Border Protection
(202) 344-3007

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Customs and Border Protection (CBP) will operate the Departure Information Systems Test in order to identify reliable and cost-effective border management capabilities that can be deployed nationwide and across multiple modes of travel. The Test will seek to test CBP's ability to verify the biometrics of departing travelers. Photos of travelers taken during boarding will be compared against photos taken previously (U.S. passport, U.S. visa, and other DHS encounters) and stored in existing CBP systems.

The Test is planned for Hartsfield-Jackson Atlanta International Airport, in Atlanta, Georgia. The Test will start on June 13, 2016, and run until September 30, 2016. One route – Atlanta to Tokyo, Japan – will be covered by the Test. However, operational developments may require CBP to relocate the test to a different flight or airport.

Prior to the departure of each flight, CBP will collect facial images and boarding pass information of all travelers, including U.S. citizens, as they pass through the passenger loading bridge to board their flight. CBP will deploy one to three cameras at or just past the departure boarding gate to capture the best possible image of the traveler's face. CBP will use this data to test the ability of CBP data systems to confirm a traveler's identity using a facial biometric comparison as the traveler departs from the United States.

Introduction

The Entry/Exit Transformation (EXT) Office is charged with developing new processes and capabilities to biometrically record the departure of non-U.S. citizens leaving the United States. EXT's strategy to accomplish its mission is based upon three primary pillars: 1) closing gaps in biographic data collection; 2) short-term targeted biometric operations; and 3) long-term transformation of entry/exit processes.

Authorities:

The 1996 Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA, Public Law No. 104-208) called for the creation of an automated system to record arrivals and departures of non-citizens at all air, sea, and land ports of entry. The 2002 Enhanced Border Security and Visa Entry Reform Act (EBSVERA, Public Law No. 107-173), the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA, Public Law No. 108-458), and the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law No. 110-53) all called for the creation of a nationwide, biometric entry/exit system.

Background:

Biometric screening on entry has been in place since 2004.[1] However, biometric screening

[1] DHS/NPPD/PIA-001 US-Visit Program, Increment 1 Privacy Impact Assessment (December 18, 2003), *available*

on exit has proved more challenging. CBP is fully committed to implementing biometric exit procedures and has launched prior field tests of biometric technologies and processes (see BE-Mobile[2] and Otay Mesa Pedestrian field tests[3]). The Secretary of the Department of Homeland Security (DHS) has committed CBP to begin deployment of biometric exit to the major U.S. international airports in FY 2018.

Test Plan:

The Departure Information Systems Test is an important step towards developing a biometric exit process and to meeting statutory and Department goals. This PIA addresses this Test, which begins on June 13, 2016, at Hartsfield-Jackson Atlanta International Airport. CBP will update this PIA, if necessary, to address any future tests as they are developed and deployed.

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).[4] 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.

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. 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 (PIAs) on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[5] and the Homeland Security Act of 2002, Section 222.[6] This PIA examines the privacy impact of the Departure Information Systems Test and collection of facial image and boarding pass biographic data as it relates to the Fair Information Practice Principles.

---

at: https://www.dhs.gov/sites/default/files/publications/pia_nppd_001_a_09142004.pdf.

[2] DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (BE-Mobile) (June 18, 2015), *available at: https://www.dhs.gov/publication/biometric-exit-mobile-air-test.*

[3] DHS/CBP/PIA-027 Southwest Border Pedestrian Exit Field Test (November 6, 2015), *available at: https://www.dhs.gov/publication/dhscbppia-027-southwest-border-pedestrian-exit-field-test.*

[4] 5 U.S.C. § 552a, *as amended.*

[5] 44 U.S.C. § 3501

[6] 6 U.S.C. § 142.

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

CBP is providing transparency to the public using signs posted in close proximity to the camera at the testing site. These signs inform the public that they will be participating in a CBP test of new technology. The signage reads as follows:

> "On this flight, U.S. Customs and Border Protection is testing new facial comparison technology during departure. We appreciate your cooperation."

Additional signage will be provided that uses iconography to show travelers how to interact with the screening device.

CBP also intends to provide notice through: a press release, informational tear sheets, fact sheets, and public announcements at the testing location to all affected travelers. Information on this and other CBP biometric field tests is available on the official CBP public website. Once the testing is complete, CBP may determine that the technology will be used at other airports. CBP will update this PIA or issue a new PIA if the Department decides to use the technology or process beyond this test. CBP is also publishing this FIPPs-based PIA to provide additional public notice.

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.

The Departure Information Systems Test will collect biometric and biographic data from all travelers, including U.S. citizens, departing through the gates where the test is in operation. As with other CBP border security procedures, participation is mandatory.

CBP is testing the algorithms and other data system abilities to perform facial image comparisons.

Identification of U.S. citizenship is an essential component of CBP exit processing. CBP believes that collection of facial images is the most effective way of differentiating between U.S. citizens and non-U.S. citizens, allowing CBP to identify any non-U.S. citizens subject to the exit requirements who may be fraudulently using a valid U.S. passport or other travel document, and thereby ensuring the accuracy of the exit data that is collected consistent with the statutory mandates. Therefore, facial images will be collected for U.S. citizens as part of this test so that

CBP can verify the identity of a U.S. citizen boarding the air carrier. Once a U.S. citizen's identity is confirmed, that biometric information will be deleted. All other travelers will have their data deleted no later than September 30, 2017, unless the data is associated with an open law enforcement matter.

CBP officers and staff will be on hand to assist travelers as needed. CBP has also created a Tear Sheet in English and Japanese that will be handed to travelers who ask for more information about the Test.

People who are denied or delayed airline boarding can file an inquiry to seek redress with the DHS Traveler Redress Inquiry Program (TRIP). Inquiries may be filed at trip@dhs.gov or at www.dhs.gov/dhs-trip.

Privacy Risk: There is a risk to individual participation because individuals cannot opt-out of the Departure Information Systems Test.

Mitigation: This risk is not mitigated. Individuals do not have the right to consent to particular uses of the information collected as part of the test due to CBP's law enforcement and other national security missions. However upon request, individuals will be provided a tear sheet to provide more information about the test. In addition, individuals may file an inquiry to seek redress with the TRIP program.

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.

In addition to the statutory authorities discussed above, the Departure Information Systems Test biometric data will be covered by the DHS/CBP-006 Automated Targeting System (ATS)[7], DHS/CBP/PIA-009 TECS system[8], and DHS/CBP-007 Border Crossing Information (BCI)[9] SORNs.

The data collected during the Departure Information Systems Test will be used by CBP to assess facial comparison capabilities (algorithm testing) and processes to confirm a traveler's identity and identify those travelers (non-U.S. citizens) who should have their departure from the

---

[7] 77 FR 30297 available at: *https://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm*
[8] 73 FR 77778 available at: *https://www.federalregister.gov/articles/2008/12/19/E8-29807/privacy-act-of-1974-us-customs-and-border-protection-011-tecs-system-of-records-notice*
[9] 80 FR 4040 available at: *https://www.regulations.gov/#!documentDetail;D=DHS-2016-0006-0001*

United States biometrically recorded. The data collected will be used for the test evaluation only, and will not be used for real-time management of airport or border security operations.

U.S. citizens must use a valid U.S. passport to enter or depart from the United States. *See* 8 U.S.C. § 1185(b). U.S. citizen data will be collected to test CBP's ability to verify a traveler's status as a U.S. citizen.

Privacy Risk: Facial images collected by the test could be used for another purpose.

Mitigation: The data collected will not be stored in CBP databases and made available for routine use in supporting CBP operations, unless it is associated with an open law enforcement matter. U.S. citizen images will be deleted upon identification and confirmation as a U.S. citizen. CBP's post-departure analysis may take up to 2 weeks to confirm the initial match identifying a traveler as a U.S. citizen. All other images will be deleted no later than September 30, 2017, unless they are associated with an open law enforcement matter.

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).

The Departure Information Systems Test will collect facial images and biographic data in the boarding pass from departing air travelers on one selected daily flight. The Departure Information Systems Test will not collect any other information from the travelers. Travelers will be instructed to place their boarding pass near the camera. This action will notify the system when to collect a proper image of the traveler.

This is a limited duration Test to determine the viability of facial comparison technology in the air exit environment. The Test will apply to one daily international flight: Atlanta to Narita Airport, Tokyo, Japan.

The collection of data from travelers will assist CBP in testing the ability to identify individuals with facial images and to determine if biometric technology can be incorporated into the airport environment without negative impacts to air carriers, airports, and the traveling public. CBP believes that collection of facial images is the most effective way of differentiating between U.S. citizens and non-U.S. citizens, allowing CBP to identify any non-U.S. citizens subject to the exit requirements who may be fraudulently using a valid U.S. passport or other travel document,

and thereby ensuring the accuracy of the exit data that is collected consistent with statutory mandates discussed above. Facial images will be collected for U.S. citizens as part of this test so that CBP can, verify the identity of a U.S. citizen boarding the air carrier.

The captured facial images and boarding pass information will not be used for enforcement checks. Biographic data from the boarding pass will be used during the evaluation to help determine the accuracy of the biometric facial matching.

The Departure Information Systems Test will run from June 13, 2016, and end no later than September 30, 2016. The data will be stored for no longer than one year after the completion of the Test, and will then be deleted, unless it is associated with an open law enforcement matter. However, if the post-test evaluation reveals an instance of identity fraud or other unlawful activity, that information will be stored in CBP systems in accordance with CBP law enforcement authorities.

Privacy Risk: This test collects PII directly from U.S. citizens who are departing the United States.

Mitigation: Once a traveler is identified as a U.S. citizen, and that match is confirmed, his or her facial image will be deleted. The Departure Information Systems Test will use electronic flight manifests to identify which individuals are scheduled to depart on the designated flight for that day. As a traveler's facial image is captured by the camera, the image will be run against the passport images of all individuals scheduled to be on the flight. Comparison occurs within the ATS database, and remains isolated from other data systems of other agencies. Confirmed U.S. citizen boarding pass information will be temporarily retained in the isolated part of ATS to support the test's evaluation. Within 1 to 2 weeks, CBP staff will manually review system generated matches related to the identification of a U.S. citizen in order to confirm that the match was correctly made. Images collected from U.S. citizens will be deleted after the match is reviewed and confirmed.

Privacy Risk: There is a risk that the test data might be stored longer than is necessary.

Mitigation: CBP will use the test data only for the evaluation, unless the data is associated with an open law enforcement record. Facial images of foreign nationals and all boarding pass information will be stored no longer than September 30, 2017. However, CBP will delete the data earlier when it is determined that the data is no longer needed. Facial images from U.S. citizens will be deleted as soon as they are identified and confirmed as a U.S. citizen listed on the specific manifest.

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.

This Test will be used to determine the viability of facial comparison technology and data system processing in the air exit environment. The collection of data from travelers will assist CBP in testing the ability to accurately identify individuals using facial images and to determine if biometric technology can be incorporated into the airport environment without negative impacts to air carriers, airports, and the traveling public. CBP will not share any of the facial image data it collects with any party outside of DHS, unless there is a legal obligation to do so.

Privacy Risk: There is a risk that data will be used beyond the scope of the test.

Mitigation: The Departure Information Systems Test does not create new records in CBP data systems. Matching results occur in an isolated part of the ATS database to support analysis of the test's results. Test data cannot be accessed by CBP operations. DHS elements outside of CBP cannot access test data. All data collected by the Departure Information Systems Test will be deleted no later than September 30, 2017, unless it is associated with an open law enforcement matter.

Privacy Risk: There is a risk that data may be inappropriately accessed.

Mitigation: Access to the data requires a login and user account password. CBP limits access to the data to cleared and designated CBP staff.

CBP staff are not permitted to manipulate, alter, erase, reuse, modify, or tamper with any facial image data. CBP takes precautions to prevent the alteration or deletion of the facial image data to ensure that all information is accurately captured and retained. The data is only stored on a CBP-approved server, which is only accessible by authorized CBP users. The data is prohibited from being downloaded, manipulated, or otherwise used for personal use.

Privacy Risk: There is a risk that the data will be used outside of CBP.

Mitigation: This test does not create new records for operational use in CBP data systems. Test data is retained in an isolated unit of the ATS database that will only support test performance analysis. Only CBP employees and contract support staff will have access to that data. All facial image data is retained in an isolated part of ATS until the conclusion of the Test's evaluation, when it will be deleted, unless it is associated with an open law enforcement matter.

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.

Facial image data is captured in real time to obtain an accurate picture of the individual. CBP officers are not permitted to manipulate, alter, erase, reuse, modify, or tamper with any facial image data during the Test. Safeguards are built into the database to prevent the alteration or deletion of the facial image data by unauthorized individuals to ensure that all information is accurately captured and retained.

The facial image data is only stored on a CBP-approved server which is only accessible by CBP, and is within the CBP firewall. All staff who access the data have had background investigations completed. The facial image data is prohibited from being downloaded, manipulated, or otherwise used for personal use. All facial image data is retained in an isolated part of ATS until the conclusion of the Test's evaluation, when it will be deleted, unless it is associated with an open law enforcement matter.

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.

The Departure Information Systems Test will store facial image photos, generate biometric templates from those photos, and store boarding pass information in the CBP data systems.

The data will be retained in an isolated part of the ATS database to evaluate how accurately CBP is able to match the facial images collected at the airport. Matching will occur against U.S. passport photographs and photographs of non-U.S. citizen visitors from their travel documents or other DHS encounters, such as a previous arrival in which a photograph was provided. CBP is responsible for data security and protection. Transmitted data will be protected with https security encryptions.

Privacy Risk: There is a risk that unauthorized individuals may see the test data.

Mitigation: The data collected cannot be viewed at the collection location (departure loading bridge) and at the time of collection. The collection device does not display the data collected. Only the CBP staff responsible for evaluating the test will see the data, and will do so only through access of isolated part of ATS database. Only individuals cleared by CBP will have access to the collection device and database.

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 persons with access to the data are required to complete annual privacy awareness training in addition to training on ethics and the CBP Code of Conduct. CBP employees and contractors must pass a full background investigation and must also be trained regarding the access, use, maintenance, and dissemination of PII before being given access to the system(s) maintaining the facial image data. Access controls are currently in place (including technological controls) to ensure authorized access to the facial image data. The facial image data will not be accessed or released for any unauthorized use. CBP will document the deletion of test data.

Privacy Risk: There is a risk that CBP staff might handle the data in an inappropriate manner.

Mitigation: Only individuals cleared by CBP will have access to the collection device and database. All CBP employees and contractors with access to the data undergo annual privacy awareness and document security training. In addition, only a limited number of staff will have access to this data, and CBP maintains logs of staff access of the data.

Conclusion

CBP conducts regular self-assessments to verify compliance with its responsibilities and the privacy risk mitigations discussed in this PIA. The DHS Privacy Office also provides ongoing guidance on all privacy issues raised by significant or new technologies and approaches. Finally, the DHS Privacy Office will be part of the process to make improvements as technology changes

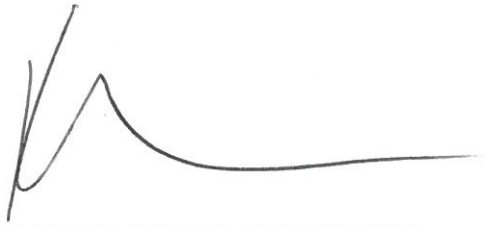
to make sure that all future technology is implemented consistent with all privacy policies, procedures, and applicable privacy laws. This PIA will be updated as CBP's methods and policies for the use of facial comparison technology evolve.

Responsible Officials

David Maher
Program Manager
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
202-344-1641

John Connors
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection
202-344-1610

Approval Signature Page



Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security