Privacy Impact Assessment Update
for the

Departure Verification System

DHS/CBP/PIA-030(a)

December 16, 2016

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

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

Abstract

In June 2016, U.S. Customs and Border Protection (CBP) published a Privacy Impact Assessment (PIA) providing notice of the Departure Information Systems Test (DIST),[1] a pilot program to test the use of facial recognition software for air passengers departing from the United States. During the pilot, CBP assessed whether air travelers' photos taken during the boarding process could be matched with photos taken previously for travel documents (U.S. passport, U.S. visa, and other DHS encounters) to provide verification of that traveler's exit from the United States. Building upon the success of this pilot, CBP is operationalizing the pilot into the Departure Verification System (DVS). CBP is publishing this PIA Update to provide a privacy assessment of the implementation of DVS, which includes two significant changes: (1) the use of facial recognition technology for additional flight routes at new airports, and (2) the use of facial comparison to create exit records for travelers departing the United States.

Overview

The 1996 Illegal Immigration Reform and Immigrant Responsibility Act[2] 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,[3] the Intelligence Reform and Terrorism Prevention Act of 2004,[4] and the Implementing Recommendations of the 9/11 Commission Act of 2007[5] all called for the creation of a nationwide biometric entry-exit system. Biometric screening on entry has been in place since 2004,[6] and CBP continues to conduct tests of various systems and processes to identify a method for comprehensive biometric exit screening, including the creation of exit records for individuals departing the United States.

Pilot Process

CBP piloted DIST to assess whether facial comparison technology could be used to confirm a traveler's exit from the United States. DIST began on June 15, 2016, at Hartsfield-Jackson Atlanta International Airport, in cooperation with a major U.S. commercial air carrier. The test was scoped to include only one route and run until September 30, 2016; the pilot was later extended through November 2016. For flights operating on this route, a CBP-manned camera and

---

[1] *See* DHS/CBP/PIA-030 Departure Information Systems Test (June 12, 2016), *available at* https://www.dhs.gov/publication/departure-information-systems-test.
[2] Pub. L. 104-208.
[3] Pub. L. 107-173.
[4] Pub. L. 108-458.
[5] Pub. L. 110-53.
[6] *See* DHS/NPPD/PIA-001 US-VISIT Program, Increment 1 (January 16, 2004), *available at* https://www.dhs.gov/sites/default/files/publications/pia_nppd_001_a_09142004.pdf.

tablet computer were placed between the boarding pass reader and the aircraft. As travelers checked in for their flight, CBP obtained passenger manifest data[7] and assembled existing traveler photographs into a downloadable file that was pushed to the tablet prior to boarding. These photographs had been accessed from various DHS and Department of State systems. As travelers passed through the boarding area, the camera took their photographs. The real-time photographs were compared to the downloaded pictures to determine if CBP systems could accurately match the two photographs. CBP used the pilot only to assess these matching capabilities; no exit records were created. Images were stored on the tablet for the duration of the flight, after which point the data was purged.

Pilot Results and Analysis

Using this matching approach, CBP was able to identify travelers with a high degree of confidence. Therefore, CBP determined that these initial findings support the piloted process as a viable solution to fulfill the mandated biometric exit requirements in certain settings. In addition, CBP received positive feedback from the airline, and the process did not substantially delay boarding. Based on these results, CBP is transitioning from test status (DIST) to operational status (DVS). DVS will expand to new airports and additional international flights. The implementation of DVS enables CBP to: 1) biometrically confirm the traveler's departure from the United States, 2) create an exit record in the traveler's crossing history, and 3) meet its mandated obligation to create a biometric entry-exit system.

Reason for the PIA Update

CBP is conducting this PIA Update to provide a privacy risk assessment and public notice that CBP is implementing DVS as a result of the success of the DIST pilot. Under DVS, CBP will collect facial images from travelers on select routes at select airports beginning in December 2016. In addition to the inclusion of new flight routes and airports, the implementation of DVS will create verified exit records for travelers on these routes, including U.S. Citizens.[8]

DVS Operational Process

DVS will follow the same process piloted by DIST. At selected departure gates at select airports, CBP will deploy a facial recognition camera in close proximity to the airline boarding pass reader. This camera will match live images with existing photos from passenger travel documents assembled based on flight manifest data of the boarding flight. Upon receipt of the passenger flight manifest and throughout the passenger check-in process, CBP will compile photos

---

[7] *See* DHS/CBP/PIA-001 Advance Passenger Information System (June 5, 2013), *available at* https://www.dhs.gov/publication/advanced-passenger-information-system-apis-update-national-counterterrorism-center-nctc.

[8] The exit records are only being created for those flights that are leaving the United States.

from the Automated Biometric Identification System (IDENT),[9] the Department of State's Consolidated Consular Database,[10] and U.S. Citizen and Immigration Service's Computer Linked Adjudication Information Management System (CLAIMS 3)[11] to build a flight-specific gallery housed in the Automated Targeting System (ATS).[12] The CBP Officer staffing the boarding gate will upload this photo gallery onto a tablet computer prior to flight boarding. At the gate, an airline operator will scan the traveler's boarding pass and the camera will take a photo of the traveler. Signage posted in close proximity to the camera will demonstrate how to interact with the device.

Once the camera captures a quality image and the system successfully matches it with a photo from the gallery associated with the manifest, the traveler will proceed to the passenger loading bridge. If the image created by the facial recognition camera system does not match the photograph on file that is associated with the individual's travel document, the operator will direct the traveler to a CBP Officer stationed at the passenger loading bridge. The CBP Officer will use a wireless handheld device[13] to verify the traveler's identity using either fingerprints for aliens (by IDENT query) or by conducting a thorough inspection to ensure the traveler is holding valid travel documents. If the CBP Officer is unable to locate a record of the traveler's fingerprints in IDENT, the officer will run a separate criminal history check in the Integrated Automated Fingerprint Identification System (IAFIS) and enroll the fingerprints in IDENT.

Once boarding is complete and CBP has verified the identity of the travelers, either through automated facial recognition or manual officer exception processing, the CBP Officer transmits the information back to ATS. CBP creates a record of the traveler's departure from the United States in the Advance Passenger Information System (APIS),[14] where the traveler record is updated from "reported" to "confirmed." CBP exit records are covered by the Border Crossing Information (BCI) system of records[15] for U.S. citizens and legal permanent residents and by the Nonimmigrant Information System (NIIS) system of records[16] for non-immigrant aliens. CBP also retains entry and exit records in the Arrival and Departure Information System (ADIS) for lawful permanent

---

[9] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (December 7, 2012), *available at* https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system.

[10] *See* Consolidated Consular Database Privacy Impact Assessment (July 17, 2015), *available at* https://foia.state.gov/_docs/PIA/ConsularConsolidatedDatabase_CCD.pdf.

[11] *See* DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems (March 25, 2016), *available at* https://www.dhs.gov/publication/dhsuscispia-016-computer-linked-application-information-management-system-claims-3-and.

[12] *See* DHS/CBP/PIA-006(d) Automated Targeting System (September 16, 2014), *available at* https://www.dhs.gov/publication/automated-targeting-system-ats-update.

[13] *See* 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.

[14] *See* DHS/CBP-005 Advance Passenger Information System, 80 FR 13407 (March 13, 2015), *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05798.htm.

[15] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016), *available at* https://www.regulations.gov/document?D=DHS-2016-0006-0001.

[16] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015), *available at* https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05804.htm.

residents and non-immigrant aliens.[17] CBP will retain non-U.S. citizen photos it collects, along with certain associated biographic information, through the DVS process in ATS. U.S. citizen photos are deleted once CBP confirms the traveler's identity. Photos stored on the tablet are purged after the conclusion of each flight.

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).[18] 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[19] and the Homeland Security Act of 2002, Section 222.[20] This PIA examines the privacy impact of the Departure Verification System and collection of facial image and boarding pass biographic data as it relates to the Fair Information Practice Principles.

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.

There has been no change to transparency since the original PIA. As CBP expands DVS, it will continue to provide notice to individuals whose facial images are captured with signs posted

---

[17] *See* DHS/CBP/PIA-024(a) Arrival and Departure Information System (March 7, 2014), *available at* https://www.dhs.gov/publication/arrival-and-departure-information-system.
[18] 5 U.S.C. § 552a, *as amended.*
[19] 44 U.S.C. § 3501 note.
[20] 6 U.S.C. § 142.

in close proximity to the camera. These signs inform the public that CBP will be capturing their photos and refers them to the CBP Info Center. In addition, CBP posts signs in boarding areas informing individuals that they may be subject to searches upon arrival or departure from the United States. These signs also include the authority and purpose for inspection, the routine uses, and the consequences for failing to provide information.

Information on this and other CBP biometric exit projects is available on the official CBP public website.[21] CBP provides additional notice to the public through this PIA Update and will publish updates or additional PIAs for future changes.

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.

Whereas DIST collected information for test purposes only, DVS will create exit records retained in CBP systems of record, including BCI, NIIS, and ADIS. Individuals seeking notification of and access to records collected during the process, or seeking to contest their content, may submit a Freedom of Information Act (FOIA) or Privacy Act request to CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, D.C. 20002
Fax Number: (202) 325-0230

Requests for information are evaluated to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

All FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process.

---

[21] *See* https://www.cbp.gov/travel/biometric-security-initiatives for more information.

Persons who believe they have been adversely impacted by this program (for example, refused boarding for transportation or identified for additional screening by CBP) may submit a redress request through the DHS Traveler Redress Inquiry Program (TRIP). DHS TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports, and train stations or at U.S. land borders. Through DHS TRIP, a traveler can request correction of erroneous data stored in DHS databases through one application. DHS TRIP redress requests can be made online at http://www.dhs.gov/dhs-trip or by mail at:

DHS TRIP
601 South 12th Street, TSA-901
Arlington, VA 20598-6901

Privacy Risk: There is a risk to individual participation because individuals cannot opt-out of participation in DVS and the creation of a CBP exit record.

Mitigation: This privacy risk cannot be fully mitigated. Although the redress and access procedures above provide for an individual's ability to correct his or her information, the only opportunity to opt-out of this program is to decline to travel. Crossing the border is considered voluntary and individuals seeking to do so are subject to the laws and rules enforced by CBP. However, upon request, individuals will be provided a tear sheet to provide more information on the project. In addition, individuals may file an inquiry to seek redress through DHS TRIP.

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.

Although the collection of DIST information was originally limited to testing purposes, the information collected under DVS will now be used for the creation of exit records, as described in the overview section of this document. CBP is publishing a new regulation to implement the systematic collection of facial images under DVS.

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).

DVS collects facial images and biographic data from the boarding pass from departing air travelers on select flights. CBP retains *facial images* for a maximum of 15 years for non-immigrant aliens and lawful permanent residents, but deletes U.S. citizen photos once their identities have been confirmed. CBP retains *biographic exit records* for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens, consistent with the BCI and NIIS System of Record Notices (SORN). Records retained in association with a law enforcement action are retained for 75 years, consistent with the TECS SORN.[22]

Privacy Risk: There is a risk that CBP may retain U.S. citizen information longer than is necessary.

Mitigation: This risk is mitigated. CBP retains exit records for U.S. citizens for a maximum of 15 years, consistent with the BCI SORN. CBP will delete facial images from U.S. citizens as soon as they are identified and confirmed as the U.S. citizen listed on the manifest. CBP will retain facial images of non-immigrant aliens and lawful permanent residents for up to 15 years in accordance with the BCI SORN.

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.

Although the collection of DIST information was limited to testing purposes, CBP will use the information it collects under DVS to create exit records, as described in the overview section of this document. CBP will share entry and exit data consistent with the terms described in the relevant SORNs listed above.

Privacy Risk: There is a risk that CBP will use exit records created under DVS for a purpose other than those specified for the original collection.

Mitigation: This risk is partially mitigated. CBP creates entry and exit records primarily in support of its mission to facilitate legitimate travel, which includes activities related to counterterrorism and immigration enforcement. However, CBP often shares information with federal, state, and local authorities, which may be authorized to use the information for purposes beyond the scope of CBP's mission. CBP provides notice of this sharing in its various SORNs, which are detailed in the original DIST PIA. CBP uses and shares information consistent with these SORNs and updates these notices for any new uses. In addition, signs in boarding areas inform individuals that they may be subject to searches upon arrival or departure from the United

[22] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008), *available at* https://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

States. These signs include the authority and purpose for inspection and the routine uses of the information gathered from those searches.

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.

There is no change to the data quality and integrity between the DIST pilot and implementation of DVS.

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.

DVS will store facial image photos, generate biometric templates from those photos, and store certain biographic information from the associated boarding pass in ATS. Matching will occur against U.S. passport photographs and photographs of non-U.S. citizens from their travel documents or other DHS encounters, such as a previous arrival into the United States in which a photograph was provided. Once the CBP Officer transmits the flight data to ATS and the flight is complete, the file is deleted from the tablet the CBP Officer uses at the departure gate. CBP uses a virtual private network (VPN) with two-factor authentication and strong encryption to transfer the data between the device and CBP systems.

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

Mitigation: This risk is mitigated. The data collected cannot be viewed at the collection location (departure loading bridge) or at the time of collection. The collection device does not display the data collected, and the images are deleted from the device after the flight is completed. Only CBP personnel and CBP contractors 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.

There has been no change impacting accountability and auditing since the DIST PIA; extensive training and access controls will remain in place for DVS.

Responsible Officials

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

Sung Hyun Ha
Program Manager
Entry/Exit Transformation Office
Office of Field Operations
U.S. Customs and Border Protection
202-344-3726

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
202-344-1610

Approval Signature Page

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