Privacy Impact Assessment Update
for the

Traveler Verification Service (TVS):

CBP-TSA Technical Demonstration

DHS/CBP/PIA-030(d)

September 25, 2017

Contact Point
Colleen Manaher
Planning, Program Analysis and Evaluation (PPAE)
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-3003

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is continuing to develop and expand its biometric entry-exit system for international flights at airports throughout the United States. In partnership with the Transportation Security Administration (TSA), CBP's latest biometric technical demonstration will use the Traveler Verification Service (TVS) cloud-based matching service to compare international travelers' photos captured by CBP against previously-captured photos. CBP is updating this Privacy Impact Assessment (PIA) to provide the public with notice regarding CBP's plans to use personally identifiable information (PII) collected by CBP devices located at TSA security checkpoints.

Overview

The 1996 Illegal Immigration Reform and Immigrant Responsibility Act[1] authorized an automated system to record arrivals and departures of non-U.S. citizens at all air, sea, and land ports of entry. CBP is collecting this information pursuant to its applicable authorities, including the 2002 Enhanced Border Security and Visa Entry Reform Act,[2] the Intelligence Reform and Terrorism Prevention Act of 2004,[3] the Implementing Recommendations of the 9/11 Commission Act of 2007,[4] and 8 U.S.C. § 1357. Although CBP has been collecting biometric information on entry since 2004,[5] CBP has continued to develop and test various systems and processes to identify a method for comprehensive biometric exit screening. Since being tasked with the biometric exit mission in 2013, CBP has been fully committed to developing and testing new processes and capabilities for using biometric information, specifically facial recognition technology, to verify the departure of persons leaving the United States. The *Consolidated Appropriations Act of 2016*[6] authorized CBP to expend up to $1 billion in certain visa fee surcharges collected over the next ten years for biometric entry and exit implementation. Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States," required DHS to "expedite the completion and implementation of a biometric entry-exit tracking system for in-scope travelers to the United States."[7]

By utilizing biometric technologies in voluntary partnerships with other federal agencies and commercial stakeholders, CBP is facilitating a large-scale transformation of air travel that will make air travel more secure, by providing increased certainty as to the identity of airline travelers

[1] Pub. L. 104-208.
[2] Pub. L. 107-173.
[3] Pub. L. 108-458.
[4] Pub. L. 110-53.
[5] *See* DHS/NPPD/PIA-001 US-VISIT Program, Increment 1 (January 16, 2004), *available at* www.dhs.gov/privacy.
[6] Pub. L. 114-113.
[7] Executive Order 13780, *Protecting the Nation from Foreign Terrorist Entry into the United States*, 82 FR 13209 (March 9, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states.

at multiple points in the travel process, and more predictable, by establishing a clear, easily-understood boarding process. The primary goal of this process, however, is to enhance the integrity of the immigration system, by better identifying which foreign nationals are violating the terms of their admission to the United States, and by providing the capability for immediate action when such violations are identified.

Previous Departure Verification Biometric Technical Demonstration Projects

In June 2016, CBP piloted the Departure Information System Test (DIST)[8] to assess whether facial comparison technology could be used to confirm a traveler's exit from the United States. During the DIST, CBP deployed a CBP-manned camera and tablet computer between the boarding pass reader and the aircraft at a departure gate in order to determine if CBP could accurately match live photographs with previous-acquired photos of the same traveler. Prior to departure, CBP downloaded passenger manifest data from the Advance Passenger Information System (APIS).[9] As travelers boarded their flight, CBP captured a photograph of each traveler and, based on the manifest of passengers scheduled to be on the flight, matched the newly-captured photo template with previously-captured photo templates downloaded from the Automated Targeting System-Unified Passenger (ATS-UPAX).[10]

Following the DIST, CBP conducted the Departure Verification System (DVS),[11] which operationalized the DIST pilot and followed the same process as the DIST. During the DVS, if the system successfully matched the traveler's photo with a photo template from the gallery associated with the manifest, the traveler proceeded to board the flight. If no match was found, a CBP Officer verified the traveler's identity through a fingerprint capture (for aliens) using a Biometric Exit (BE)-Mobile wireless handheld device[12] and a query in the Automated Biometric Identification System (IDENT).[13] Alternatively, the CBP Officer conducted an inspection to ensure the validity of the individual's travel documents. If the CBP Officer was unable to locate an IDENT fingerprint record, the officer ran a separate criminal history check in the Federal Bureau of Investigation's (FBI) Next Generation Identification[14] (formerly Integrated Automated Fingerprint Identification System (IAFIS)) and enrolled the fingerprints into IDENT. As CBP verified the identity of the travelers, either through automated facial recognition or manual officer processing, the CBP

[8] *See* DHS/CBP/PIA-030 Departure Information Systems Test (June 13, 2016), *available at* www.dhs.gov/privacy.
[9] *See* DHS/CBP/PIA-001 Advance Passenger Information System (June 5, 2013), *available at* www.dhs.gov/privacy.
[10] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at* www.dhs.gov/privacy.
[11] *See* DHS/CBP/PIA-030(a) Departure Verification System (December 16, 2016), *available at* www.dhs.gov/privacy.
[12] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (June 18, 2015), *available at* www.dhs.gov/privacy.
[13] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (December 7, 2012), *available at* www.dhs.gov/privacy.
[14] *See* Privacy Impact Assessment: Next Generation Identification (NGI) (February 20, 2015), *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

Officer returned the results to the respective CBP systems.

Traveler Verification Service

Similar to operations of the DVS, the TVS[15] uses CBP's biographic APIS manifest data[16] and existing photographs of all travelers boarding international flights to confirm the identity of the traveler, create an exit record, and biometrically confirm the exit of in-scope non-U.S. citizens.[17] ATS-UPAX generates biometric templates of the historical images of travelers for a given flight and temporarily stores them in the Virtual Private Cloud (VPC)[18] prior to boarding. These images include photographs captured by CBP during the entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters.[19]

As boarding begins, each international traveler approaches the departure gate to present a boarding pass and stands for a photo in front of a camera, which is owned either by CBP or by a partner airline or airport authority.[20] In either case, the camera securely transmits usable images to CBP's cloud-based TVS facial matching service.[21] The matching service generates a template from the departure image and uses that template to search the historical photo templates for all travelers on that particular international flight manifest. The TVS returns faces that best match the reference face, thus verifying the identities of individual travelers. If a match is found, the traveler proceeds to the aircraft, and the TVS returns the positive results, along with the respective unique identifier

[15] *See* DHS/CBP/PIA-030(b) Traveler Verification Service (TVS) (May 15, 2017), *available at* https://www.dhs.gov/privacy.

[16] The manifest, which contains information collected by airlines and transmitted to CBP prior to departure, consists of biographic information such as name, date of birth, country of citizenship, passport information (number, country of issuance and expiration date), and an airline-generated alphanumeric unique ID (UID). Either the travel agent, travel website hosting service, or the airline generates the UID at the time of the reservation. The UID is comprised of a sequential number (which is only valid for the particular airline and the specific flight), plus the Record Locator, a six-digit code used to access additional information about the traveler. The APIS manifest also includes specific details of the traveler's itinerary, such as flight number, carrier, originating airport, and destination airport.

[17] There is the requirement to biometrically confirm the departure of "in-scope" travelers. An "in scope" traveler is any person who is required by law to provide biometrics upon exit from the United States pursuant to 8 CFR 235.8; *see also* 8 CFR 235.1(f)(ii). Additionally, it is generally unlawful for a U.S. citizen to depart from the United States without a valid U.S. passport; *see* Immigration and Nationality Act (INA) § 215(b) (8 U.S.C. § 1185(b)).

[18] CBP uses a commercial Virtual Private Cloud (VPC) that is a logically isolated (walled-off) virtual network over which CBP administers control.

[19] U.S. passport and visa photos are available via the Department of State's Consular Consolidated System. *See* Privacy Impact Assessment: Consular Consolidated Database, *available at* https://2001-2009.state.gov/documents/organization/93772.pdf. Other photos may include those from DHS apprehensions or enforcement actions, previous border crossings, and immigration records.

[20] Although CBP supplies cameras for the TVS initiative at specified airports and departure gates, in some cases, under a recent initiative described in DHS/CBP/PIA-030(c) Traveler Verification Service (June 12, 2017), *available at* www.dhs.gov/privacy, airlines and airport authorities voluntarily deploy and operate the cameras. Based on their pre-arranged agreements with CBP, the camera technology provided by these stakeholders must meet CBP's technical specifications to capture facial images of travelers and use the TVS matching service for identity verification. Each camera is connected to the TVS, sometimes through an authorized integration platform or vendor, via a secure, encrypted connection.

[21] CBP's cloud-based backend facial matching service received an Authority to Test on May 24, 2017.

(UID), to ATS-UPAX. If, however, after repeated attempts, the TVS cannot verify the identity of the traveler, a CBP Officer escorts the traveler to verify his or her identity using alternative methods. Similar to the DVS, CBP creates a record of the traveler's departure in APIS, which updates the traveler record from "reported" to "confirmed."

Reason for the PIA Update

CBP is publishing this updated PIA because CBP and TSA are forming a partnership to develop and implement a biometric technical demonstration using the TVS cloud-based matching service.[22] This new initiative will test the accuracy and utility of placing cameras at the TSA security screening checkpoint, rather than at the airline's departure gate, which has been the camera location for previous demonstration projects. CBP and TSA's partnership is a multi-phased approach. The first phase, which is addressed in this PIA Update, involves the collection of biometrics using CBP-owned equipment under CBP authorities. The purpose of the first phase is to determine the viability of fulfilling CBP's biometric exit responsibility using the TVS to verify travelers' identities at a different location, the TSA checkpoint.

Similar to other versions of the TVS, Phase I of the CBP-TSA project will use CBP's biographic APIS manifest data and existing photographs of all travelers boarding international flights at the specified terminal. This phase will be limited to three TSA podiums (screening checkpoints) at one specified international airport terminal for up to 60 days from the planned start date. At the beginning of each day, APIS will load flight manifests for all international flights at the specified terminal scheduled throughout the day. For each of the travelers scheduled for international flights, ATS-UPAX will generate biometric templates of travelers' historical images from previous passports, visas, and other DHS encounters. Those templates will be temporarily stored in the TVS VPC.

When travelers who are scheduled for outbound international flights reach the TSA Travel Document Checker (TDC) podium, the TDC will direct the travelers to a CBP-owned facial recognition camera to scan their boarding pass and pose for a photo.[23] Because this test is limited to one specified international airport terminal, all travelers who approach the TSA podium are expected to be international travelers. The TSA screening process will remain unchanged. The TDC will continue to check the traveler's travel and identity documents using TSA's current identity verification process. The TSA TDC will visually verify the traveler's boarding pass, and will also direct the traveler to look into the CBP-owned camera. Once the photo is captured, it will be converted into a template and shared, along with associated metadata from the traveler's boarding pass scan,[24] with the TVS backend cloud-based matching service. The TVS then matches

[22] *See* DHS/CBP/PIA-030(c) Traveler Verification Service (June 12, 2017), *available at* www.dhs.gov/privacy.
[23] TDCs will be trained on the cameras. Although CBP owns the cameras, TDCs will be operating them.
[24] This metadata, which is sent from the camera, includes the carrier code, flight number, departure port, and departure date as well as the optional token, which in this case would be the boarding pass scan.

the newly-captured photo template against numerous galleries of the templates of historical images of travelers for all international flights at the specified terminal on that particular day temporarily stored in the VPC, and returns the results of the match, along with the associated UID.

The primary difference in the CBP-TSA demonstration project's matching process, as opposed to the process outlined in the previous TVS updates, is that each template will be matched against multiple galleries, based on that day's flight manifests for that particular international terminal, rather than being matched against the templates for only one departing flight's manifest. Additionally, during Phase I of this CBP-TSA project, following the capture and matching, the TDC will continue to check a passenger's travel and identity documents before allowing the traveler to proceed through the regular screening process and onto the flight, regardless of the results of the facial recognition match (positive or negative), provided the traveler does not require further screening by TSA for other reasons. Neither the TDC nor a CBP Officer will adjudicate non-matches or inconclusive results during this demonstration. In such cases, the TDC will use TSA's current processes for identity verification. During previous technical demonstrations, CBP Officers used alternative methods to adjudicate non-matches and inconclusive results.

DHS-branded signage in plain view near the TSA checkpoint, along with tear sheets as requested, will communicate CBP's request that outbound international travelers permit themselves to be photographed, along with instructions, opt-out procedures, and Frequently Asked Questions. If travelers do not wish to participate in the facial recognition proof of concept at any time during the process, they will be allowed to opt-out and continue through normal TDC procedures.

Through this technical demonstration, CBP and TSA are testing and evaluating the viability of using facial recognition technology at the TSA checkpoint; this demonstration will not create exit records. However, CBP will continue to retain biographic exit records from the boarding pass in the Arrival and Departure Information System (ADIS)[25] for lawful permanent residents and non-immigrant aliens, consistent with the ADIS System of Records Notice (SORN).[26] 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 Border Crossing Information (BCI)[27] and Nonimmigrant Information System (NIIS)[28] SORNs, respectively. Records associated with a law enforcement action are retained for 75 years in accordance with the TECS SORN.[29]

All newly-captured photos and templates will be deleted from ATS-UPAX within 14 days and will be deleted from the VPC no later than the conclusion of the flight. During this two-week

[25] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* www.dhs.gov/privacy.
[26] *See* DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2005).
[27] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[28] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015).
[29] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

period, CBP may temporarily retain photos within the isolated part of ATS-UPAX,[30] consistent with the ATS SORN, in order to support system audits, to evaluate the TVS facial recognition technology, and to ensure accuracy of the facial recognition algorithms. CBP will conduct biometric analysis, using the photos, the gallery, and information from the boarding pass, to determine match rates and the performance and viability of this process in order to recommend any necessary updates for subsequent phases of the project. CBP staff will also manually review system-generated matches for all U.S. citizens to confirm the match.

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).[31] 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 PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[32] and the Homeland Security Act of 2002, Section 222.[33] This PIA Update examines the privacy impact of the TVS and collection of facial images by devices located at the TSA screening checkpoint as they relate 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 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.

As CBP expands the TVS, CBP is working closely with TSA to post DHS-branded signs in close proximity to the TSA checkpoint. These signs will provide the required notice to travelers of CBP's collection near the TSA checkpoint and use of information under this initiative, in addition to opt-out procedures. Upon request, TDCs or CBP Officers will provide CBP/TSA-

[30] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[31] 5 U.S.C. § 552a, *as amended.*
[32] 44 U.S.C. § 3501 note.
[33] 6 U.S.C. § 142.

approved tear sheets to individuals with additional information on the project, including CBP's legal authority to implement the program and the purposes for collecting the data, the routine uses of the information collected, and the option to decline participation in the project.

Information on this and other CBP biometric exit projects is available on the official CBP and TSA public websites. CBP will also issue a press release and update its websites as CBP deploys new biometric processes at new airports.[34] Finally, CBP and TSA provide additional notice to the public through this PIA Update and will publish updates or additional PIAs for future changes.

Privacy Risk: There is a risk that travelers will not know their photographs are being taken for testing purposes.

Mitigation: This risk is mitigated. Signs posted in close proximity to the TSA checkpoint provide the public with timely notice that CBP will capture their photos for testing purposes. These signs will refer travelers who have questions related to the TVS to the CBP Info Center, a TDC, or CBP Officer, who will provide CBP/TSA-approved tear sheets with Frequently Asked Questions, opt-out procedures, and additional information. These tear sheets will also include the legal authority for CBP to implement the program and the purposes for collecting the data, and the routine uses of the information collected. In addition, this PIA and the CBP website will provide general notice to the public about CBP's collection near the TSA checkpoint and use of information under this initiative.

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.

For purposes of this demonstration project, the TVS will rely upon information collected directly from the individual by CBP at the TSA checkpoint as well as additional information collected from the airline (via the APIS manifest) and photographs collected previously from CBP, DHS, or the Department of State. Under Phase I of this CBP-TSA project, all passengers, including those who request not to participate and those with a non-match or inconclusive facial recognition matching result, will still be required to have identity and travel documents verified by the TSA TDC before the traveler is allowed to proceed through the regular checkpoint screening process and onto the flight. Neither non-matches nor inconclusive facial recognition results will be adjudicated at the checkpoint. Again, the TDC officer will continue to follow standard TSA processes for identity and travel document verification.

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

Individuals seeking notification of and access to biometric images 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
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20002
Fax Number: (202) 325-1476

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.

Persons who believe they have been adversely impacted by this program may submit a redress request through 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 that individuals are not aware of their ability to make record access requests for records collected pursuant to the CBP-TSA partnership.

Mitigation: This risk is partially mitigated. This PIA and the relevant SORNs describe how individuals can make access requests under FOIA or the Privacy Act for CBP records collected under its partnership with TSA. In addition, the tear sheets and signage will refer travelers to the CBP website, where they may find information on requesting their information.

U.S. law does not extend Privacy Act protections to individuals who are not U.S. citizens or lawful permanent residents, except to the extent such a request is the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law.

In addition, providing individual access and/or correction of records may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records collected and retained pursuant to the TVS process, regardless of a subject's citizenship, could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

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 primary purpose of the TVS has not changed since the publication of the previous TVS PIA Update, DHS/CBP/PIA-030(c).[35] The information collected by CBP under its partnership with TSA will be used to verify travelers' identities, as described in the "Overview" section of this document. Although CBP has previously collected biographical PII from the airlines through the APIS manifest, the collection of travelers' images at the TSA checkpoint will expedite identity verification and ultimately enhance security. In addition to issuing this PIA, CBP is updating its regulation to address the systematic collection of biometrics from all travelers, including U.S. citizens and lawful permanent residents, at ports of entry throughout the country under the TVS.

Privacy Risk: There is a risk of travelers confusing CBP's border security mission with TSA's domestic transportation security mission and assuming CBP mission creep.

Mitigation: This risk is partially mitigated. DHS-branded signage, which will be placed in plain view near the TSA checkpoint, along with tear sheets as requested, will provide notice regarding the partnership between CBP and TSA. In addition, the signs and tear sheets will communicate CBP's request that outbound international travelers permit themselves to be photographed, along with instructions, opt-out procedures, and Frequently Asked Questions. Finally, the CBP website, this PIA, and associated SORNs will provide notice of CBP's partnership with TSA for a technical demonstration on biometric exit.

Privacy Risk: There is a risk of travelers assuming that the TSA TDCs are verifying immigration status for domestic air travel.

Mitigation: This risk is mitigated. This PIA, along with the DHS-branded signage, tear sheets, and the CBP website will clearly explain that this technical demonstration project being implemented for international flights only. Additionally, this particular terminal is recognized as

[35] *See* DHS/CBP/PIA-030(c) Traveler Verification Service, *available at* https://www.dhs.gov/privacy.

an international flights terminal and is operated by an international carrier. Currently, there are only international flights departing or arriving at this terminal. In the future, the only occasion that a flight may depart from this terminal and land in a U.S. city would be rare occurrence that this flight connects in a U.S. city in route to an international destination.

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 TVS collects facial images and biographic data from departing air travelers on select flights. CBP is working with TSA to collect the photo images at the TSA checkpoint with CBP-owned equipment under CBP authorities. The TVS matching service converts the photos into secure templates and matches them against templates of previously-captured images. CBP retains the image templates for up to 14 days in ATS-UPAX for the newly-captured photos for the purposes of reviewing and confirming the match, evaluating the facial recognition technology, ensuring accuracy of the algorithms, and supporting system audits. By the conclusion of each flight, CBP will delete all facial images from the VPC. CBP will continue to retain 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[36] and NIIS[37] SORNs, respectively. However, records retained in association with a law enforcement action are retained for 75 years, consistent with the TECS SORN.[38] TSA will not access or retain any information under this initiative.

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 facial images for U.S. citizens collected during this technical demonstration in ATS-UPAX only as long as necessary, but for no longer than two weeks, for the purposes outlined above. CBP maintains only biographical departure information on U.S. citizens for up to 15 years, in accordance with the BCI SORN. Immediately following the flight departure, ATS-UPAX will send a message to the VPC that the flight has departed. At that point, and no later than immediately after the conclusion of the flight, the VPC will delete the facial images of all travelers whose identities on the flight manifest have been verified.

Privacy Risk: There is an overcollection risk that CBP may collect photos from individuals at the TSA checkpoint who are not departing on an international flight.

[36] See DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[37] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015).
[38] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

Mitigation: This risk is mitigated by the fact that CBP and TSA are deploying this technical demonstration at a checkpoint dedicated to international flights. All travelers screened at this checkpoint are boarding international flights, for which CBP and TSA have collected APIS manifests.

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.

During the first phase of this technical demonstration, CBP will use the information it collects under the TVS to assess the feasibility of capturing images at the TSA checkpoint rather than the departure gate, as described in the "Reason for the PIA Update" section above. CBP will not create exit records during this demonstration but will continue to share biographical entry and exit data as normal, consistent with the terms described in the relevant SORNs listed above. TSA will not access or retain information under this initiative.

Privacy Risk: There is a risk that CBP will use the photos captured under the TVS at the TSA checkpoint for a purpose other than those specified for the original collection.

Mitigation: This risk is partially mitigated. CBP is collecting the images during this technical demonstration only to test the viability of satisfying its biometric exit responsibility and verifying departing travelers' identities at the TSA checkpoint. CBP captures photos of travelers at the checkpoint and shares them with the TVS via a secure, encrypted connection. CBP shares the images, in the form of irreversible photo templates, with the VPC for the purpose of matching travelers with previous photos and thus verifying their identities. CBP requires the VPC to delete all photos no later than the conclusion of the flight. During this phase of the demonstration, regardless of the results of the match, the TDC will verify identity and travel documents through the normal screening process.

On occasion, CBP may also share information with federal, state, and local authorities, which may be authorized to use the information for purposes beyond the scope of CBP's mission for law enforcement, judicial proceedings, congressional inquiries, audits, and other lawful purposes. CBP provides notice of this sharing in its various SORNs, which are cited here and also detailed in the previous PIAs. CBP uses and shares information consistent with these SORNs and updates these notices for any new uses.

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.

In general, the practices for ensuring data quality and integrity are the same as discussed

in the previous TVS PIAs. CBP applies the same technical specification requirements in this initiative, the purpose of which is to test whether TVS can be deployed effectively at an earlier point in the travel process. Although the traveler photos will be matched against a larger gallery of photos than in previous TVS initiatives (*i.e.*, the gallery will contain photos from multiple flights, rather than just the flight being boarded at a particular gate), CBP expects that this change will not negatively impact the accuracy or match rate.

Privacy Risk: There is a risk that the TVS match rate will be less successful against a larger gallery (*i.e.*, photos of travelers from multiple flights).

Mitigation: This risk is mitigated. Because this is a technical demonstration that will have no impact on the traveler's ability to board, and because CBP is not creating exit records based on this initiative, there are no privacy risks posed by the increased volume of photos in the gallery.

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.

There are no changes impacting security since the most recent PIA Update. CBP will store TVS information in secure CBP systems and temporarily in a secure VPC environment,[39] using biometric templates that cannot be reverse engineered for viewing by external parties. Like previous TVS iterations, CBP uses strong HTTPS/SSL encryption to transfer the data between the camera, the VPC, and CBP systems as well as for PII at rest. Only authorized CBP and TSA personnel will have access to the collection device, and only authorized cloud service provider (CSP) personnel will have access to the cloud database. While TDCs will be stationed near the cameras and will direct the passengers to pose for the photos, they will not be able to access or share individual images. Additionally, although CSP personnel may technically access the database, they will not have the keys to decrypt the data.

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 are no changes to auditing and accountability process from the previous PIA. CBP access controls, including technological controls, will ensure only authorized access to the facial image data. The facial image data will not be accessed or released for any unauthorized use. No data is archived within TVS. Once match results are returned to ATS-UPAX, all flight data - photos and match scores - are deleted from TVS. In addition, CBP does not retain match information

[39] CBP's cloud-based backend facial matching service received an Authority to Test on May 24, 2017.

longer than 14 days. CBP will document the deletion of data from UPAX and the CSP. Encryption keys are stored using the CSP's Key Management Service, on hardware hosted by the CSP. This Key Management Service is a FedRAMP-compliant service that fully audits every time a key is used. The keys are managed by the TVS administrators. The CSP's auditing services allow the TVS to monitor every time the key is accessed programmatically.

Responsible Officials

Colleen Manaher
Executive Director
Planning, Program Analysis and Evaluation
Office of Field Operations
U.S. Customs and Border Protection
202-344-3003

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

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security