Privacy Impact Assessment Update
for the

Traveler Verification Service (TVS): Partner Process

DHS/CBP/PIA-030(c)

June 12, 2017

Contact Point
Kim A. Mills
Planning, Program Analysis and Evaluation (PPAE)
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

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. CBP is partnering with commercial air carriers and airport authorities that will capture facial images of travelers as part of their business processes, and then send those photographs to CBP for use in the Traveler Verification Service (TVS). CBP will match the images against previously-captured photos by using a cloud environment. 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 airlines and airport authorities, and CBP's use of facial matching technology in a cloud environment.

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. The 2002 Enhanced Border Security and Visa Entry Reform Act,[2] the Intelligence Reform and Terrorism Prevention Act of 2004,[3] and the Implementing Recommendations of the 9/11 Commission Act of 2007,[4] all called for the creation of a nationwide biometric entry-exit system. Although biometric screening on entry has been in place since 2004,[5] CBP has continued to develop and test various systems and processes to identify a method for comprehensive biometric exit screening, including the creation of exit records for all individuals, regardless of citizenship, departing the United States. Since being tasked with the biometric exit mission in 2013, CBP has been fully committed to developing and testing new processes and capabilities for biometrically recording persons leaving the United States through the use of facial recognition technology. 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]

---

[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.

By partnering with stakeholders on a voluntary basis and using biometric technologies, CBP is facilitating a large-scale transformation of air travel that will make air travel: (1) more secure, by providing increased certainty as to the identity of airline travelers at multiple points in the travel process; (2) more predictable, by establishing a clear, easily-understood boarding process, and (3) able to build additional integrity to 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 that occurs.

Previous Departure Verification Pilots

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. As travelers checked in for their flight, CBP used a manned camera to take a photograph of each traveler prior to boarding and matched the photograph to previously downloaded passenger manifest data from the Advance Passenger Information System (APIS).[9] CBP compared the real-time photographs with the expected travelers' downloaded biometric (photo) templates to determine if CBP could accurately match live photographs with previous-acquired photos of the same traveler.

Following the DIST, CBP conducted the Departure Verification System (DVS),[10] 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 the passenger loading bridge. If no match was found, the operator directed the traveler to a CBP Officer, who used a wireless handheld device[11] to verify the traveler's identity using a fingerprint capture (for aliens) and a query in the Automated Biometric Identification System (IDENT),[12] or 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[13] (formerly Integrated Automated Fingerprint Identification System (IAFIS)) and enrolled the fingerprints into IDENT. As CBP verified the identity of the

---

[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-030(a) Departure Verification System (December 16, 2016), *available at* www.dhs.gov/privacy.
[11] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (BE-Mobile) (June 18, 2015), *available at* www.dhs.gov/privacy.
[12] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* www.dhs.gov/privacy.
[13] *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.

travelers, either through automated facial recognition or manual officer processing, the CBP Officer transmitted information back to the respective CBP systems.

Reason for the PIA Update

CBP is publishing this updated PIA because the recently initiated TVS[14] is expanding to allow commercial air carriers and select airport authorities ("partners") to provide their own facial recognition cameras and capture the images of travelers consistent with their own business processes and requirements (for example, to use facial images instead of paper boarding passes). Commercial air carriers and airport authorities that provide cameras for their own business purposes may now opt-in to the TVS process. These partners will capture the traveler images consistent with their business purposes, and then transmit the photos they capture to CBP through a connection with CBP's cloud-based TVS. CBP does not capture the photos directly from the traveler under this TVS expansion.

Commercial air carriers and airport authorities have an incentive to provide their own camera and use CBP facial matching technology to improve the capabilities of airline personnel to verify traveler identities, resulting in faster and more secure boarding, and to streamline the traveler's departure process.

Traveler Verification Service

Similar to operations of the DVS, the TVS[15] uses CBP's biographic APIS manifest data[16] and existing photographs of U.S. citizen and non-U.S. citizen 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] Under the TVS, the Automated Targeting System-Unified Passenger (ATS-UPAX)[18] generates biometric templates of the historical images of travelers for

[14] *See* DHS/CBP/PIA-030(b) Traveler Verification Service (TVS) (May 15, 2017), *available at* https://www.dhs.gov/privacy.
[15] *Id.*
[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). The UID is generated by either the travel agent, travel website hosting service, or the airline 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 § 215(b) (8 U.S.C. § 1185(b)).
[18] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at* https://www.dhs.gov/privacy.

a given flight and temporarily stores them in the Virtual Private Cloud (VPC)[19] 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.[20] As boarding begins, each traveler approaches the departure gate to present a boarding pass and stands for a photo in front of a CBP-owned camera, which is connected to the VPC via a secure, encrypted connection. A sign (see sample in Appendix A) placed near the camera in the boarding area provides notice that CBP is capturing travelers photos to verify their identities and create exit records.

Once the camera captures a usable image, it submits the image to CBP's cloud-based backend facial matching service via an HTTP/SSL-encrypted connection.[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 manifest. The matching service returns faces that best match the reference face, thus verifying the identities of individual travelers. If a match is found between the newly-captured image template and the pool of previously-captured image templates, a light signals the match, and CBP (or in some cases, a trained representative from the airline or airport) directs the traveler to proceed to the aircraft. If the camera is unable to capture a satisfactory image within a reasonable amount of time, the traveler is required to stand for another photo. If, after repeated attempts, the identity of the traveler cannot be verified, a CBP Officer escorts the traveler from the immediate area and attempts to verify his or her identity using alternative methods.

As CBP verifies the identity of the travelers, either through automated facial recognition or manual officer exception processing, the backend matching service returns the "match/no-match" results, along with the respective associated UID, to ATS-UPAX. Similar to the DVS, CBP creates a record of the traveler's departure from the United States in APIS, which updates the traveler record from "reported" to "confirmed." CBP also retains entry and exit records in the Arrival and Departure Information System (ADIS)[22] for lawful permanent residents and non-immigrant aliens, consistent with the ADIS System of Records Notice (SORN).[23] 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 Border Crossing Information (BCI)[24] and Nonimmigrant Information System (NIIS)[25] SORNs, respectively. However, records

[19] CBP uses a commercial Virtual Private Cloud (VPC) that is a logically isolated (walled-off) virtual network over which CBP administers control.
[20] 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.
[21] CBP's cloud-based backend facial matching service received an Authority to Test on May 24, 2017.
[22] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* https://www.dhs.gov/privacy.
[23] *See* DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2005).
[24] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[25] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015).

associated with a law enforcement action are retained for 75 years, consistent with the TECS SORN.[26]

CBP temporarily retains all photos within the isolated part of ATS-UPAX to support system audits, to evaluate the TVS facial recognition technology, and to ensure accuracy of the facial recognition algorithms. All newly-captured photos and templates will be deleted from ATS-UPAX within 14 days but will be deleted from the VPC no later than after the conclusion of the flight. CBP staff manually reviews system-generated matches for all U.S. citizens to confirm the match.

CBP Partnerships with Commercial Air Carriers and Airport Authorities

Generally, the TVS will continue to operate as described above and in the previous TVS PIA Update.[27] The airlines must continue to provide the manifest information for a particular flight to APIS, and the cloud-based matching service will match that particular flight's gallery of relevant photo templates (which in many cases are linked with the respective UIDs) against the newly-captured photo templates. However, while CBP will continue to supply cameras for the TVS initiative at specified airports and departure gates, this PIA Update describes a new CBP initiative to facilitate partnerships with approved airlines and airport authorities. A number of airlines and airport authorities, some of which are already incorporating the use of traveler photographs into their own business processes, may opt to leverage their own technology in partnership with CBP to facilitate identify verification. Based on pre-arranged agreements with CBP, these stakeholders will deploy their own camera operators and camera technology meeting CBP's technical specifications to capture facial images of travelers and utilize the TVS matching service for identity verification. Each camera will be connected to the VPC via a secure, encrypted connection.

The photo capture process may vary according to the unique requirements of each participating airline and airport authority, in partnership with CBP. During boarding, each traveler will stand for a photo in front of a partner-provided camera. Aided by the authorized airline or airport personnel, the partner-owned camera will attempt to capture a usable image and will submit the image, sometimes through an authorized integration platform or vendor, to CBP's cloud-based TVS facial matching service. TVS will then generate a template from the departure photo and use that template to search the assembly of historical photo templates in the VPC. Some airlines will continue to accept boarding passes at the gate, while other carriers will accept CBP's biometric identity verification in lieu of boarding passes as part of a new paperless, self-boarding process.

As the identity of the traveler is verified, the matching service will return the "match/no-match" results, often along with the respective UID, to ATS-UPAX and to the respective airline or airport authority. Generally, the traveler will be allowed to proceed to the aircraft following a successful match between the newly-captured image template and the pool of previously-captured

[26] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[27] *See* DHS/CBP/PIA-030(b) Traveler Verification Service, *available at* https://www.dhs.gov/privacy.

image templates. If, after repeated attempts, the identity of the traveler cannot be verified, a CBP Officer may be contacted to verify identity using alternative methods.

Similar to the TVS, CBP will create a record of the traveler's departure from the United States in APIS, which updates the traveler record from "reported" to "confirmed." CBP will retain entry and exit records as described above and consistent with the BCI,[28] NIIS,[29] and ADIS[30] SORNs. CBP recommends that the partners, along with their authorized integration platform, retain the matching results for no longer than 14 days. In some cases, partners may retain the newly-captured photos taken with their own cameras for longer, if required for their business processes. Airline and airport authorities that do not require short-term retention for business purposes will not use or retain the photos.

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 image and boarding pass biographic data as it relates to the FIPPs.

---

[28] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[29] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015).
[30] *See* DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2005).
[31] 5 U.S.C. § 552a, *as amended.*
[32] 44 U.S.C. § 3501 note.
[33] 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.

As CBP expands the TVS, CBP will work closely with the respective air carriers and airport authorities to post signs (see Appendix A) in close proximity to the partner-provided cameras and operators. These signs will provide the required notice to travelers whose facial images are captured. Because crossing the border is considered voluntary, travelers are subject to the laws and rules enforced by CBP. When the departure photos are captured, these signs inform the public that the partner organization will share the photos with CBP. Travelers who have questions related to TVS will be referred to the CBP Info Center. In addition, CBP will post signs in boarding areas informing individuals that they may be subject to inspection by CBP, and the purpose for such inspections, upon arrival or departure from the United States. Upon request, the airlines and airport authorities who provided the camera technology will provide CBP-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 consequences for failing to provide the information.

Information on this and other CBP biometric exit projects is available on the official CBP public website. CBP will also issue press releases and update its website as it deploys new biometric processes at new airports.[34] Finally, CBP provides 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 submitted to CBP and used for departure verification.

Mitigation: This risk is mitigated. This PIA, along with signs posted in close proximity to the cameras and operators (see Appendix A) inform the public that the respective airline or airport authority will capture their photos and share them with CBP, and then will refer travelers who have questions related to TVS to the CBP Info Center. In addition, the airlines and airport authorities will provide CBP-approved tear sheets to travelers who request additional information on the project. These sheets will include the legal authority for CBP to implement the program and the purposes for collecting the data, the routine uses of the information collected, and the consequences for failing to provide the information. This PIA and the CBP website provide general notice to the public about CBP's collection and use of information under this initiative.

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

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 TVS relies upon information collected directly from the individual by the respective airlines and airport authorities (*i.e.*, the photograph captured during the boarding process), 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 CBP's partnerships with airlines and airport authorities, agreements between CBP and the partner organization will guide opt-in/opt-out procedures. For some participating airlines, for instance, a traveler may request not to participate in the TVS and instead present credentials to airline personnel before proceeding through the departure gate. In other cases, if an individual opts-out of TVS, his or her identity may be verified by an available CBP Officer who will manually verify the traveler's identity and the authenticity of the documentation. If, in this scenario, the officer is concerned about identity of the individual or the document, he or she may swipe the individual's passport through a Biometric Exit (BE) Mobile[35] device and conduct a more complete inspection, as appropriate.

The TVS will create exit records retained in CBP systems of records, 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
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.

[35] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (June 28, 2015), *available at* https://www.dhs.gov/privacy.

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 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 may be denied boarding if they refuse to submit to biometric identity verification under the TVS.

Mitigation: This privacy risk is partially mitigated. Although the redress and access procedures above provide for an individual's ability to correct his or her information, the only way for an individual to ensure he or she is not subject to collection of biometric information when traveling internationally is to refrain from traveling. Individuals seeking to travel internationally are subject to the laws and rules enforced by CBP and are subject to inspection. If a traveler, however, requests not to participate in the TVS, specified agreements between CBP and the partner airline or airport authority will guide opt-in or opt-out procedures. For some participating airlines, a traveler may request not to participate in the TVS and instead present credentials to airline personnel before proceeding through the departure gate. In other cases of an opt-out, an available CBP Officer may employ manual processing to verify the individual's identity. 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.

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 TVS partner process.

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 the records that CBP receives from the partner airlines. CBP cannot provide redress for any business uses by the partner airlines that may impact the traveler experience.

Redress is available for U.S. citizens and lawful permanent residents through requests made under the Privacy Act as described above. 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(b).[36] The information collected by CBP partners under the TVS will be used to verify travelers' identities and create exit records, 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 by commercial air carriers and airport authorities will expedite identity verification and enhance security. Also, in some cases, airlines will accept CBP's identity verification and facial matching in lieu of requiring the presentation of boarding passes, resulting in enhanced efficiencies for the airlines and their customers. 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 that commercial air carriers will use the photographs for purposes beyond departure verification.

Mitigation: This risk cannot be fully mitigated. Commercial air carriers are not collecting photographs on CBP's behalf or under CBP authorities. The air carriers are collecting images pursuant to their contractual relationship with the travelers and may use the photographs consistent with that authority.

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

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 specified partners, such as commercial air carriers and airport authorities, who will collect the images of travelers and share the images with the TVS, often through an integration platform or other vendor. The TVS matching service converts the photos into secure templates and matches them against templates of previously-captured images. For CBP partners and their approved vendors or integrators who retain the images in line with their business purposes and processes, signed Memoranda of Understanding (MOU) with CBP will govern their retention practices. CBP recommends that its partners delete the matching results within 14 days, and encourages them to delete the newly-captured photos as soon as they are no longer needed for business purposes. However, once the images are shared with CBP, the airline or airport authority, along with their approved integrator or vendor, may choose to retain the newly-captured photos consistent with their contractual relationship with the traveler. This practice mirrors CBP's retention policy of up to 14 days in ATS-UPAX for the newly-captured photos, linked with their respective UIDs, 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[37] and NIIS[38] SORNs, respectively. However, records retained in association with a law enforcement action are retained for 75 years, consistent with the TECS SORN.[39]

Privacy Risk: There is a risk that the airline or airport partner will retain biometric information longer than is necessary.

Mitigation: This risk cannot be fully mitigated. CBP cannot limit the time that approved airlines or airport partners can retain information collected for their own business purposes. The MOUs in place between the airlines or airport partners and CBP govern retention practices. CBP recommends that its partners delete the matching results within 14 days, and encourages them to delete the newly-captured photos as soon as they are no longer needed for business purposes.

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

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.

CBP will use the information it collects through its public and private sector partners under the TVS 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 the TVS for a purpose other than those specified for the original collection.

Mitigation: This risk is partially mitigated. CBP collects information under this process in order to verify the identities of travelers departing the United States; however, CBP uses border crossing information more broadly. CBP creates entry and exit records primarily in support of its mission to facilitate legitimate travel and enforce immigration laws, which include activities related to counterterrorism and immigration enforcement. CBP partners such as select air carriers and airport authorities capture photos of travelers and share them with the TVS via an authorized integration platform or other vendor. 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 that the VPC delete all photos after the flight has departed, and not later than when the flight has concluded. 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. 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.

Privacy Risk: There is a risk that approved partners will use biometric images collected under the TVS for a purpose other than identity verification.

Mitigation: This risk cannot be fully mitigated. Under the TVS-partners initiative, industry partners collect photographs consistent with their contractual relationships with the travelers and voluntarily provide them to CBP in support of this project. The original collection is subject to the contract between the industry partner and the traveler, to which CBP is not a party. Questions regarding a particular partner's use of biometric images it may collect to facilitate the program should be directed to the relevant industry partner.

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.

CBP uses biometric technologies to meet the need for ensuring accurate, relevant, timely, and complete identity verification for travelers. In order to enhance the accuracy of matching, CBP has developed technical specification requirements for participating airlines and airport authorities and their vendors because the quality of facial images dramatically impacts the performance of all facial recognition algorithms. The National Institute of Standards and Technology (NIST) has shown that the accuracy (true acceptance rate, or TAR) of a picture captured in a well-controlled environment, such as a passport photo, is of significantly higher quality than for a picture taken in an unstructured environment (for example, with a poor quality web cam). CBP requires facial images captured at the departure gate to conform closely to the International Civil Aviation Organization (ICAO) standards (ISO 19794-5)[40] and the American National Standard for Information (ANSI)/NIST-Information Technology Laboratory (ITL) 1-2011: Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information.[41]

CBP regularly tests the accuracy of its photo matching algorithms to achieve the highest possible accuracy. CBP's testing has illustrated that high-quality facial images that meet the specifications above result in good match performance. CBP requires an accuracy goal of 96% TAR for facial images acquired in an airport/seaport exit environment. CBP expects the TVS partner cameras to: (1) capture multiple images; (2) draw the traveler's attention to the camera, and hold the traveler's attention throughout the capture process; (3) include a "time-out" function in order to send the best-captured image of the traveler if no image was able to meet the desired quality threshold; and (4) provide proper lighting.

In order to continually improve upon the quality of the images, the DHS Science and Technology Directorate (S&T) assists CBP in testing the effectiveness of various commercial, academic, and government algorithms in matching facial photographs. S&T is generating a report identifying how each algorithm performed as a true positive rate, false positive rate, false match rate, and false non-match rate.

Privacy Risk: There is a risk that the cameras provided by either the air carrier or airport authority will be unable to capture images of high enough quality to produce accurate matches, resulting in CBP's inability to confirm traveler identities.

Mitigation: This risk is mitigated. CBP requires its partners' cameras to meet ANSI/NIST and international standards as well as an accuracy goal of 96% TAR. In addition, the cameras are required to: (1) capture multiple images; (2) draw the traveler's attention to the camera and hold

[40] For more information, please *see* https://www.iso.org/standard/50867.html.
[41] For more information, please *see* http://fingerprint.nist.gov/standard/.

the traveler's attention throughout the capture process, and alter the traveler's position when the process is complete; (3) include a "time-out" function in order to send the best-captured image of the traveler if no image was able to meet the desired quality threshold; and (4) provide proper lighting. If, for any reason, the identity of the traveler cannot be verified after repeated attempts, a CBP Officer may be called on to verify identity using alternative methods. During manual processing, an officer manually verifies the authenticity of the documentation, such as the passport, and manually verifies that the traveler matches the passport. If the officer is concerned about the authenticity of the document(s) and/or the identity of the individual, he or she may swipe the passport through a Biometric Exit (BE) Mobile[42] device.

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.

CBP will store TVS information in secure CBP systems and temporarily in a secure VPC environment,[43] once the partner organization shares the newly-captured image with CBP. ATS-UPAX creates biometric templates of each of the historical photos, as well as the newly-captured exit photos in order to secure the photos for matching and storage. Biometric templates are strings of multiple numbers that represent specified images and facilitate facial recognition matching within a secure environment. These templates cannot be reverse engineered for viewing by external parties. CBP uses a virtual private network (VPN) with two-factor authentication and 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 representatives of the approved CBP partners will have access to the collection device, and only CBP staff and cloud service provider (CSP) personnel may have access to the cloud database. Although CSP personnel may technically access the database, they will not have the keys to decrypt the data.

The CSP selected for this initiative will adhere to the security and privacy controls required by NIST Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing,"[44] and the DHS Chief Information Officer. CSP Encryption keys are stored using the CSP's Key Management Service, 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. The CBP Office of Information

[42] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (June 28, 2015), *available at* https://www.dhs.gov/privacy.
[43] CBP's cloud-based backend facial matching service received an Authority to Test on May 24, 2017.
[44] *See* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

and Technology (OIT) has conducted an initial security review of the VPC and approved the system for interim deployment; a full security review will follow within six months.

Privacy Risk: There is a risk that unauthorized individuals may view the photos in the VPC database.

Mitigation: This risk is mitigated. The photos collected cannot be viewed at the collection location (departure loading bridge) or at the time of collection. CBP creates a template of each historical image as well as each newly-captured photo upon exit. These photo templates cannot be reverse-engineered for viewing photos, and the images are deleted from the VPC no later than the conclusion of the flight. Only authorized representatives of the approved CBP partners will have access to the collection device, and only CBP staff and the CSP personnel may have access to the cloud database. Although CSP personnel may technically access the database, they will not have the keys to decrypt the data. In addition, CBP uses strong encryption, both at rest and in transit.

Privacy Risk: There is a risk of breach of the nongovernment equipment used to store the template images that is designed for secure storage for security vetting purposes.

Mitigation: This risk partially mitigated. The TVS cloud environment is operating under a temporary "Authority to Test" until a full security authorization process is completed. CBP uses strong HTTPS/SSL encryption in order to secure the data both at rest and in transit, such as during the data transfers between the cameras, the cloud, and CBP systems. Despite these precautions, there remains some risk of an unauthorized user gaining access to the data in the VPC; however, additional controls mitigate the potential for harm. The VPC houses only a biometric template, which cannot be reverse engineered for viewing by unauthorized users; accordingly, any data accessed in an unauthorized fashion would be unrecognizable and unusable. In addition, although CBP cannot fully mitigate the security risks inherent due to the temporary storage of photos on IT infrastructure provided by all of its partners, CBP requires its partners to encrypt the biometric data, both at rest and in transit. Finally, to ensure that proper security controls have been implemented, CBP will conduct a full security review of the entire TVS infrastructure and network within six months of approval of this PIA Update.

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.

CBP access controls, including technologic 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. CBP encourages partners not retain match

information longer than 14 days. Moreover, 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.

Privacy Risk: There is a risk to auditing and accountability because CBP cannot dictate security or auditing requirements to the airline and airport partners.

Mitigation: This risk is mitigated. The CBP Privacy Office will conduct a CBP Privacy Evaluation[45] within one year of launch to ensure that all parties, including airlines, airport authorities, and cloud providers, are in compliance with the required privacy protections. All PII is encrypted at rest and in transit. The CSP's FedRAMP-compliant Key Management Service creates an audit trail every time an encryption key is used. Finally, the CSP's auditing services allow the TVS to monitor the dates and times the encryption 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 Page

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

_____

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

[45] The results of the CBP Privacy Evaluation will be shared with the DHS Privacy Office.

APPENDIX A: Sample Sign with Privacy Notice

Posted at Airport Departure Gates

(near Partner-Operated Cameras):

[CBP Partner] is collecting facial images and sharing them with CBP to verify each traveler's identity and to create a record of departure from the United States. For more information, please visit our website at www.cbp.gov.

APPENDIX B: Sea Entry Process

Updated July 6, 2018

Beginning in July 2018, U.S. Customs and Border Protection (CBP) is working with commercial partners to biometrically verify the identities of passengers arriving on sea cruise vessels. Using the Traveler Verification Service (TVS) Partner Process described in the body of this PIA, CBP and its partners aim to make travel more secure while enabling CBP to comply with biometric entry-exit program requirements.

Under this process, CBP generates an Advance Passenger Information System (APIS) manifest of passengers scheduled to board a particular cruise. Based on the APIS manifest, CBP compiles a gallery of historical photos from DHS holdings. The APIS manifest, which contains information collected by airlines and transmitted to CBP prior to departure, consists of biographic information such as the name, date of birth, country of citizenship, passport information (number, country of issuance, and expiration date), and an airline-generated alphanumeric unique ID (UID). The manifest also includes specific details of the traveler's itinerary, such as flight number, carrier, originating airport, and destination airport. The APIS information is screened against TECS Records and other law enforcement databases in order for CBP to ascertain if any security or law enforcement risks exist. Once the vessel arrives at the U.S. Port of Entry (POE), cruise lines employ cameras to collect facial photographs of passengers as they debark. The cruise line submits the photograph to the CBP TVS cloud matching service, which creates a template of the photo and perform facial matching against the gallery of historical photo templates described above. If the matching process returns a positive result, CBP indicates to cruise personnel that it has verified the traveler's identity.

Travelers for whom the matching process returns a negative result are directed to a CBP Officer for inspection. U.S. Citizens may choose to inform the cruise line that they do not wish to participate in the photo collection process. Instead, they will submit to an alternative inspection performed by a CBP Officer. Signage and optional tear sheets will be provided for travelers who are U.S. Citizens to inform them that they have the voluntary option to inform the cruise line that they do not wish to participate in the photo collection process and would rather be inspected by a CBP Officer. Once CBP allows the traveler to proceed, the traveler advances to egress through the Federal Inspection Services (FIS) area. CBP then confirms the traveler's arrival and updates the traveler record from "reported" to "confirmed" in APIS and creates an arrival record in the CBP systems outlined in this PIA.

Privacy Impact Assessment

Transparency

CBP will operate the same principles of transparency as under the air partner process. CBP will work closely with its partners to post signs and provide tear sheets notifying travelers of the purpose of this initiative and where to find more information. Travelers who have questions related to TVS will be directed to the CBP Info Center. Information on this and other CBP biometric exit projects is available on the official CBP public website. Finally, CBP provides additional notice to the public through this PIA Update and will publish updates or additional PIAs for future changes.

Individual Participation

CBP involves the individual in its collection of PII, and provides procedures for requesting alternative processing, in the same manner as the air partner process. The TVS relies upon information collected directly from the individual by the respective partners (*i.e.*, the photograph captured during the boarding process), as well as additional information collected from the carrier (via the APIS manifest) and photographs collected previously from CBP, DHS, or the Department of State. CBP and its partners provide alternative processing procedures for U.S. Citizens who request it.

Principle of Purpose Specification

The purpose of the TVS sea entry partner process is consistent with the air exit partner process described earlier in this PIA. The information collected by CBP partners under the TVS will be used to verify travelers' identities and create border crossing records. Although CBP has previously collected biographical personally identifiable information (PII) from partners through the APIS manifest, the collection of travelers' images by commercial carriers will expedite identity verification and enhance security.

Principle of Data Minimization

CBP's expansion of the TVS partner process to the sea environment will result in an increase in the data it collects from the traveling public. In an effort to mitigate the impacts of this expanded collection, CBP seeks to minimize the data it retains by deleting facial images within the time periods outlined earlier in this PIA. CBP recommends that its partners delete the matching results within 14 days and encourages the partners to delete the newly-captured photos as soon as they are no longer needed for business purposes. However, once the images are shared with CBP, the partner, along with their approved integrator or vendor, may choose to retain the newly-captured photos consistent with their contractual relationship with the traveler. CBP deletes the photos from the TVS cloud matching service within six hours of the conclusion of the cruise and does not retain U.S. Citizen photographs under this initiative.

Principle of Use Limitation

CBP will use the information it collects through its public and private sector partners under the TVS to create border crossing records, as described earlier in this PIA. CBP will only share entry and exit data consistent with the terms described in the relevant SORNs listed above.

Principle of Data Quality and Integrity

CBP has developed technical specification requirements for participating airlines and airport authorities and their vendors because the quality of facial images dramatically impacts the performance of all facial recognition algorithms. CBP regularly tests the accuracy of its photo matching algorithms to achieve the highest possible accuracy. CBP's testing has illustrated that high-quality facial images that meet the specifications above result in good match performance.

Principle of Security

As with the air exit process described earlier in this document, CBP stores TVS information in secure CBP systems and temporarily in a secure Virtual Private Cloud (VPC) environment, and uses a virtual private network with two-factor authentication and 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 representatives have access to the collection device, and only CBP staff and cloud service provider personnel may have access to the cloud database.

Principle of Accountability and Auditing

As with the air exit process, CBP's programmatic and technologic controls ensure that only authorized access to the facial image data. Further, CBP deploys auditing tools within its systems to ensure appropriate retention and deletion of data in accordance with the policies and procedures outlined in this PIA.