Privacy Impact Assessment
for the

# Traveler Verification Service

## DHS/CBP/PIA-056

## November 14, 2018


**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 congressionally mandated to deploy a biometric entry/exit system to record arrivals and departures to and from the United States. Following several years of testing and pilots, CBP has successfully operationalized and deployed facial recognition technology, now known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. CBP has issued Privacy Impact Assessments (PIA) documenting each new phase of TVS testing and deployment. CBP is now issuing this comprehensive PIA to a) consolidate all previously issued PIAs and b) provide notice to the public about how TVS collects and uses personally identifiable information (PII). CBP is conducting this overarching, comprehensive PIA for the TVS that will replace all previous PIAs and provide a consolidated privacy risk assessment for TVS.

# Overview

The 1996 Illegal Immigration Reform and Immigrant Responsibility Act[1] authorized the U.S. Government to use an automated system to record arrivals and departures of non-U.S. citizens at all air, sea, and land ports of entry. CBP is also authorized to collect biometric entry and exit information pursuant to numerous laws, including 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] Although CBP has been collecting biometric information on entry since 2004,[5] in 2013 CBP began 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]

Perhaps the most challenging aspect to deploying a nationwide biometric entry/exit system is the myriad differences in logistics and locations where travelers depart the United States. Even

[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.

limited to the air environment only, each airport authority is different and manages its departure gates in different ways. CBP's collection of biometrics for entry and exit processing poses a number of logistical challenges. First, CBP Officers (CBPO) must process a large volume of travelers in a relatively short period. Second, although infrastructure exists to conduct thorough traveler inspections upon entry to the United States, there has not been such an infrastructure for outbound travelers. Third, the collection of biometrics is a privacy-sensitive practice, with heightened concern on behalf of U.S. citizens, and outbound travelers who are not accustomed to CBP inspection at exit. CBP must tackle these practical challenges with the congressional mandate to implement a comprehensive biometric entry/exit program.

In addressing these challenges, CBP spent several years testing various technologies in various locations to determine which technology could be deployed large-scale without disrupting legitimate travel and trade, while still meeting the biometric exit mandate.

*Early Test Deployments*

In June 2016, CBP piloted the Departure Information System Test (DIST)[8] to assess whether facial comparison technology could confirm a traveler's exit from the United States. CBP operated DIST at Hartsfield-Jackson Atlanta International Airport, in cooperation with a major U.S. commercial airline, and scoped the test to include only one route and to operate until November 2016. For flights operating on this route, CBP placed a CBP-manned camera and tablet computer between the boarding pass reader and the aircraft. As travelers checked in for their flight, CBP used passenger manifest data from the Advance Passenger Information System (APIS)[9] and generated biometric templates from existing traveler photographs, which had been assembled on the tablet prior to boarding. As travelers passed through the boarding area, the camera took their photographs. CBP compared the real-time photographs with the expected travelers' downloaded biometric (photo) templates downloaded from the Automated Targeting System-Unified Passenger (ATS-UPAX),[10] to determine if CBP systems could accurately match live photographs with previously-acquired photos of the same traveler. CBP created no exit records but simply used the pilot to assess these matching capabilities. CBP stored the images on the tablet for the duration of the flight and then purged the photos.

The initial findings from DIST supported the process as a viable solution to fulfilling the mandated biometric exit requirements in certain settings. In addition, the airline provided positive feedback to CBP, and the process did not substantially delay boarding. Based on these results,

---

[8] *See* DHS/CBP/PIA-030 Departure Information Systems Test (June 13, 2016), *available at* https://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.

CBP's Departure Verification System (DVS)[11] operationalized the DIST process and expanded to a number of additional international flights at new airports. DVS allowed CBP to biometrically confirm each traveler's departure from the United States and create an exit record in the traveler's crossing history. 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 Officer returned the results to the respective CBP systems. CBP conducted full PIAs to assess the privacy risks of both the DIST and the DVS, and to provide notice to the public about CBP's ongoing tests of biometric exit technologies.

In 2017, CBP operationalized the process piloted under the DIST and DVS under a new name, TVS, which marked the expansion of facial recognition for biometric exit to seven additional airports, as well as the collection of data for operational use.

In this context, facial recognition has presented CBP with the best biometric approach because it can be performed relatively quickly, with a high degree of accuracy, and in a manner perceived as less invasive to the traveler (e.g., no actual physical contact is required to collect the biometric). This approach, as with all biometric collections, poses privacy risks which, as discussed below, are mostly mitigated. Nevertheless, CBP's phased deployment has shown the use of facial recognition technology is successful in a variety of scenarios that meet CBP's business requirements while requiring minimal infrastructure investments and space redesign and minimal impacts on travelers. Moreover, the phased deployment has allowed CBP to ensure that biometrics are collected, maintained, and used consistent with privacy laws and best practices.

---

[11] *See* DHS/CBP/PIA-030(a) Departure Verification System (DVS) (December 16, 2016), *available at* https://www.dhs.gov/privacy.
[12] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Program (July 5, 2018), *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.

## Traveler Verification Service

The TVS is an accredited CBP information technology system that consists of a group of similar systems and subsystems that support the core functioning and transmission of data between CBP applications and partner interfaces.[15] CBP will use the TVS as its backend matching service for all biometric entry and exit operations that use facial recognition, regardless of air, land, or sea. Previously, CBP had considered using different technologies based on the different environments in which an individual could present themselves for inspection or exit the United States, but CBP has determined that the TVS facial matching service works across all CBP operating environments (air, land, and sea).

*Biometric Galleries*

Regardless of the method of entry or exit, e.g., pedestrian, vehicle, cruise ship, vessel, or airplane, the TVS system conducts the backend biometric matching and provides a result to different CBP systems depending on the environment. For all biometric matching deployments, the TVS relies on biometric templates generated from pre-existing photographs that CBP already maintains, known as a "gallery." These images may include photographs captured by CBP during previous entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters.[16]

[15] Two IT systems under the Federal Information Systems Management Act (FISMA), the TVS and TVS-Internal (TVS-I) Systems, provide similar biometric cloud matching services for CBP entry and exit processing. However, to simplify the privacy compliance coverage, this PIA covers both the TVS and TVS-I Systems and their subsystems, referring to both systems as the TVS.

[16] 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.

CBP builds "galleries" of photographs based on where and when a traveler will enter or exit. If CBP has access to advance passenger manifest information, the CBP will build galleries of photographs based on upcoming flight or vessel arrivals or departures. If CBP does not have access to advance passenger information, such as for pedestrians or privately owned vehicles at land ports of entry, CBP will build galleries using photographs of "frequent" crossers for that specific port of entry, taken at that specific port of entry, that become part of a localized photographic gallery.

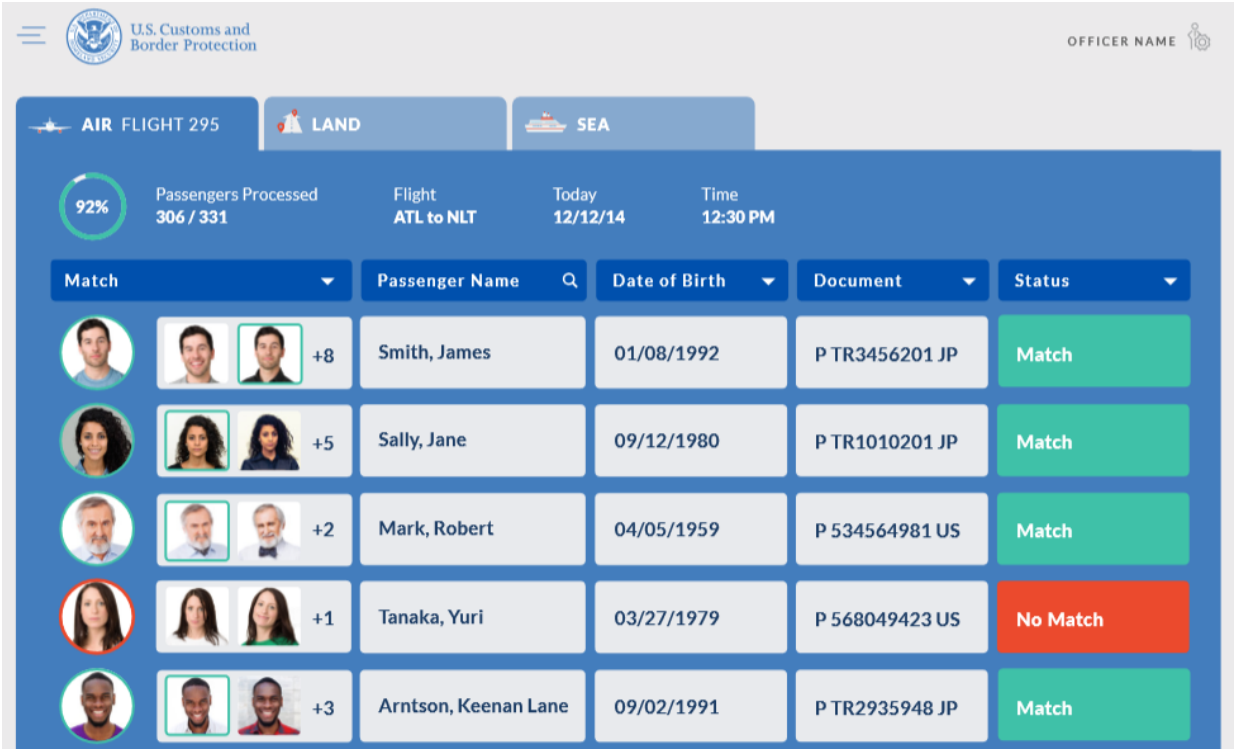


Figure 1. TVS uses biographic advanced passenger information system (APIS) manifest data and existing photographs (previous CBP encounters, U.S. Passport, U.S. Visa) to build a flight gallery. Then TVS matches the "live photograph" taken prior to boarding with images from the gallery associated with the manifest to create a confirmed departure.

CBP creates localized photographic galleries using either Advance Passenger Information System (APIS)[17] data or CBP-generated lists of frequent travelers at a specific port of entry. To populate the localized galleries with photographs, CBP compiles photographs from existing CBP sources from the Automated Targeting System (ATS)[18] Unified Passenger Module (UPAX)

[17] *See* DHS/CBP/PIA-001 Advance Passenger Information System (June 5, 2013), *available at* https://www.dhs.gov/privacy and DHS/CBP-005 Advance Passenger Information System, 80 FR 13407 (March 13, 2015).
[18] *See* DHS/CBP/PIA-006 Automated Targeting System (January 13, 2017), *available at* https://www.dhs.gov/privacy.

system. TVS will then generate biometric templates[19] for each gallery photograph and store the template, but not the actual photograph, in the TVS virtual private cloud (VPC)[20] for matching when the traveler arrives or departs.

*Collection Process*

Due to the complexities in logistics across the entry and exit environments, CBP will collect photographs of the arriving or departing traveler via several different iterations depending on the local port of entry. When the traveler presents him or herself for entry, or for exit, the traveler will encounter a camera connected to CBP's cloud-based TVS facial matching service via a secure, encrypted connection. This camera matches live images with existing photo templates from passenger travel documents. The camera may be owned by CBP, the air or vessel carrier, another government agency (e.g., the Transportation Security Administration (TSA)), or an international partner. Once the camera captures a quality image and the system successfully matches it with historical photo templates of all travelers from the gallery associated with that particular manifest, the traveler proceeds to inspection for admissibility by a CBP Officer, or exits the United States.

CBP owned and operated cameras: CBP has deployed CBP owned and operated cameras in almost all traveler processing scenarios to test TVS. CBP owned and operated cameras, which were initially used only in the air exit environment, are now being deployed for the biometric collection and matching via the TVS in the air entry, land, and sea entry environments as well. In the air environment, the major difference between CBP-operated cameras and airline or partner operated cameras is that in locations in which CBP operates the cameras, CBP Officers are present to verify identity manually with a wireless BE-Mobile handheld device.[21] TVS deployment for processing arriving air travelers mirrors the process for air exit, with manifest-based galleries and a similar facial recognition algorithm, but integrates it into CBP's entry inspection applications.

Inbound and outbound processing for travelers on commercial sea vessels (e.g., cruise ships) will resemble the air entry and exit processes, as this travel method is also based on a passenger manifest.

While CBP may create APIS manifests on land border crossers via bus or rail, unlike travelers in the air and sea environments, there are no manifests created for pedestrian travelers to assemble a gallery of known travelers. CBP is developing processes that would enable the use of TVS at the land border; for example, CBP may briefly retain local galleries of travelers who have

[19] A biometric template is a digital representation of a biometric trait of an individual generated from a biometric image and processed by an algorithm. The template is usually represented as a sequence of characters and numbers. For the TVS, templates cannot be reverse-engineered to recreate a biometric image. The templates generated for the TVS are proprietary to a specific vendor's algorithm and cannot be used with other vendor's algorithms.
[20] CBP uses a commercial Virtual Private Cloud (VPC) that is a logically isolated (walled-off) virtual network over which CBP administers control.
[21] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Program (July 5, 2018), *available at* https://www.dhs.gov/privacy.

recently crossed at a given Port of Entry and are expected to cross again within a given period of time.

Carrier owned and operated cameras: 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 identity verification. In compliance with CBP's business requirements, these stakeholders deploy their own camera operators and camera technology meeting 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 via a secure, encrypted connection. While the photo capture process may vary slightly according to the unique requirements of each participating airline and airport authority, the IT infrastructure supporting the backend process is the same. Please see Appendix B for a full list of up-to-date CBP commercial partnerships and deployments.


Figure 2. British Airways deployment of "eGates" facial recognition technology in partnership with CBP at Orlando International Airport.

Other government Agency-owned and operated cameras: CBP has been working with the Transportation Security Administration (TSA) to test the TVS process for verifying traveler identities using the TVS camera technology and matching services at the TSA security screening checkpoint. Standard TSA security screening procedures have required manual identity checks by the TSA Transportation Security Officers (TSO). A recent technical demonstration, which served as a variation of the TVS exit process, leveraged the technologies to automate what has typically been a manual identity verification process for travelers. This demonstration used the APIS manifest data to create a gallery of travelers scheduled to board specified outbound international flights during a defined period. The primary difference in the CBP-TSA matching process, as opposed to the process outlined with CBP owned and operated cameras, 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. The CBP-TSA matching process is only deployed for international travelers and does not impact individuals traveling on domestic flights. Please see Appendix C for a full list of up-to-date CBP and other government Agency partnerships and deployments.

International partner owned and operated cameras: CBP is developing global biometric partnerships in order to share facial images, as appropriate, in order to enhance security and

expedite international travel. CBP will leverage biometric data collected by a partnering country's arrival process and use the shared information to record a biometric exit from the United States, thus facilitating the ability to confirm a biometric departure without major investments in infrastructure. These partnerships are also helpful in the arrivals context. This initiative can be particularly useful for CBP in verifying the identity of first-time Visa Waiver Program[22] travelers, for whom CBP has no photo available. By obtaining a photo in advance of travel from the international partner, CBP can verify the identity of the traveler upon arrival. CBP is developing programs with select international airlines and foreign countries, in which the international partner may collect the photos of travelers to the United States at the airport of origin and securely transmit the facial images to CBP. Please see Appendix D for a full list of up-to-date international partnerships and deployments.

For a full description of each collection method, and an up-to-date list of deployments, please see the Appendices of this PIA.

*Retention and Storage*

With the operational deployment of TVS, CBP transmits facial images for in-scope travelers[23] to IDENT for retention as the traveler's biometric encounter with CBP. DHS already retains all entry photos of in-scope travelers in IDENT in order to create biometric records of entry for those travelers. In addition, retaining exit photos ensures that CBP can access up-to-date photos of in-scope travelers for more accurate future matching through the TVS. Since 2004, CBP has collected biometric information in the form of fingerprints and a facial photo on entry for in-scope travelers; CBP transmits this information to IDENT, where it is stored in association with a Fingerprint Identification Number (FIN).[24] Each FIN is associated with individual encounters (EID), which represent each interaction between that individual and an IDENT data provider. These encounters include the face image, full name, and gender (which comes from the document

[22] The Visa Waiver Program enables most citizens or nationals of participating countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. For more information, see https://travel.state.gov/content/travel/en/us-visas/tourism-visit/visa-waiver-program.html.

[23] 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 235.1(f)(ii). "In-scope" travelers include any alien other than those specifically exempt as outlined in the CFR. Exempt aliens include: Canadian citizens under section 101(a)(15)(B) of the Act who are not otherwise required to present a visa or be issued a form I-94 or Form I-95; aliens younger than 14 or older than 79 on the data of admission; aliens admitted A-1, A-2, C-3 (except for attendants, servants, or personal employees of accredited officials), G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visas, and certain Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas unless the Secretary of State and the Secretary of Homeland Security jointly determine that a class of such aliens should be subject to the requirements of paragraph (d)(1)(ii); classes of aliens to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or an individual alien to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply.

[24] *See* DHS/USVISIT-004 Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007).

number and is not collected by CBP). CBP does not store facial images voluntarily collected from U.S. citizens under this initiative in IDENT, as U.S. citizens are not considered in-scope.[25]

During the initial phases of the DIST, DVS, and TVS technical demonstration, photos of U.S citizens were retained for a limited period of time. During the 2017 deployment of the TVS, for instance, facial images of U.S. citizens as well as in-scope immigrants were maintained for up to 14 days in ATS-UPAX for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. However, CBP does not retain the images of U.S. citizens once their identities are verified by TVS.[26] Only photos of non-U.S. citizens are retained for the full 14 days in ATS-UPAX and for the full retention period in IDENT. In addition, within 12 hours, CBP purges all photos, regardless of immigration or citizenship status, from the TVS cloud matching service. Retention is described in more detail in section 5 of this PIA.

***TVS Privacy Risk Assessment***

As with all biometric modalities, facial recognition poses a unique set of privacy issues. Facial images can be captured at a distance, covertly, and without consent. Further, facial images are ubiquitous, and whereas individuals may take measures to avoid fingerprint and iris collection, there are fewer ways to hide one's face. The newness of the technology, and differences in reliability for certain demographics in previous applications, raise the bar for testing to ensure that matching algorithms are effective. CBP is taking steps to promote data minimization and privacy protections by using an airline-generated alphanumeric unique ID (UID)[27] and other methods to disassociate the biographic information associated with the new facial images, and populating the record with test biographic "dummy" information. The algorithms have continued to improve their performance over time.

CBP has also taken a number of steps to ensure that its deployment of the TVS is consistent with the following privacy best practices:

*Opt-out provisions:* U.S. citizens who do not wish to submit to facial photo capture pursuant to these processes may request alternative processing, which typically involves a manual review of their travel documents by a CBPO. Prior to admission into the United States, the CBPO must ensure that the traveler is a U.S. citizen, lawful permanent resident, or is otherwise eligible

---

[25] CBP does not retain U.S. citizen photos in IDENT pursuant to the entry/exit processes discussed in this PIA. However, pursuant to existing procedures and in accordance with its authorities, CBP transmits photos to IDENT for individuals in the Trusted Traveler network, including U.S. citizens. *See* DHS/CBP/PIA-002 Global Enrollment System (GES): Trusted Traveler Program System (August 15, 2017), *available at* www.dhs.gov/privacy.

[26] Photos of all travelers, including U.S. citizens, are held in secure CBP systems for no more than 12 hours after identity verification, in case of an extended system outage.

[27] 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.

for entry, and that the traveler is not attempting to import or export any merchandise in violation of U.S. laws. Similarly, CBPOs may inspect travelers departing the United States in order to create exit records and as required for law enforcement operations. CBP posts information on opt-out procedures near the point of collection.

*Deletion of U.S. citizen photos:* Once a match is made and notated in the appropriate systems, U.S. citizens' photos are retained for no more than 12 hours in the TVS cloud for disaster recovery purposes, then deleted. CBP retains only a confirmation of the crossing and the associated biographic information. No photos of U.S. citizens are retained under this process.

Using the TVS enables CBP to biometrically confirm the traveler's arrival and updates the traveler record from "reported" to "confirmed" in APIS. CBP also retains entry and exit records in ADIS for lawful permanent residents and non-immigrant aliens. Transmission of photos to IDENT for in-scope travelers will begin upon publication of this PIA. Since the commencement of the TVS in early 2017, CBP has retained the historical photos of travelers as well as the photo templates of newly-captured images within ATS/UPAX. From the beginning of the TVS initiative in early 2017, all newly-captured photos for non-U.S. citizens were deleted from ATS/UPAX within 14 days and deleted from the TVS cloud-matching service no later than after the conclusion of the flight. No photos are permanently stored in the TVS cloud matching service.

Once the TVS matching process is complete, and the response is returned, the facial images of U.S. citizens are immediately deleted from the TVS. CBP does not retain any photos collected from U.S. citizens pursuant to this process. Under the CBP partner process as implemented in the business requirements, CBP does not allow its approved partners such as airlines, airport authorities, or cruise lines to retain the photos they collect for their own business purposes. These partners must immediately purge the photos following transmittal to the TVS. The CBP partner's system must allow CBP to audit compliance with this requirement.[28]

*Routine testing:* As technology continues to shift and progress, CBP needs baseline data to test across technology providers over time. CBP regularly tests its facial matching algorithms to ensure high performance and maximize match rates while reducing the risk of false positives. CBP has continued to explore the best modalities and collection methods for implementation of the biometric entry/exit program. In particular, CBP continues to conduct testing and analysis to determine the factors that lead to high quality biometric capture that will result in higher confidence scores. A number of technical demonstrations over the last several years have provided CBP with a baseline of images collected in a live environment that may be compared with images collected in other similar CBP demonstrations. Throughout this process, CBP has designed the

[28] If an approved partner elects to capture photos with their own cameras for their own business purposes under a separate process, that partner must provide separate notice, such as signage, which does not link that particular process to CBP. Along these lines, as of the publication data of this PIA, no airline or airport authority had communicated to CBP any plans to capture and retain biometric data at the departure gate for its own purposes.

tests in order to assess whether the process generates the same results across all demographics, including differences in skin tones. CBP's efforts to ensure the reliability and quality of its biometric matching algorithm is outlined in more detail in Section 2 of this PIA.

Due to the large volume of travelers and border crossers, it would not be practical for CBP to use formally-generated frontal head-on facial images, such as are taken for a driver's license or passport. Rather, CBP is increasingly employing technologies that do not require subjects to present their face directly to the camera. Given this new focus, technology providers are continuing to refine their solutions to collect face images with minimal participation from the subject. While a more streamlined capture of facial images (rather than a "stop and look" approach) poses operational benefits to CBP, it also poses increased privacy risks since the individual may be unaware that their photo is being captured. CBP is committed to ensuring that as technology continues to advance, it provides timely and meaningful notice to individuals of its collection of biometric information. These efforts are described in section 4 of this PIA.

# Section 1.0 Authorities and Other Requirements

## 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Pursuant to its mission to secure the United States border, CBP has general authority to conduct searches and detentions at the border, including: 8 U.S.C. §§ 1225 and 1357; 19 U.S.C. §§ 482, 507, 1461, 1496, 1499, 1581, 1582, 1589a, and 1595a; 22 U.S.C. § 401; and 31 U.S.C. § 5317, as well as the attending regulations of CBP promulgated at Titles 8 and 19 of the Code of Federal Regulations.

The data collected under the TVS is authorized by CBP's general statutory authority, including the following statutes and regulations:

- Homeland Security Act of 2002;[29]
- Tariff Act of 1930, as amended;[30]
- Aviation and Transportation Security Act of 2001;[31]
- Section 103(a)(1) of the Immigration and Nationality Act (INA) of 1952, *as amended*;[32]

[29] Pub. L. 107-296, 116 Stat. 2135.
[30] 19 U.S.C. §§ 66, 1433, 1459, 1485, 1624, 2071.
[31] Pub. L. 107-71, 115 Stat. 597.
[32] 8 U.S.C. § 1103(a)(1), to enforce and administer the immigration laws (as defined in 101(a)(17) of the INA) with respect to matters within the jurisdiction of CBP.

- Title 8 of the United States Code, Aliens and Nationality;[33]
- 18 U.S.C. Chapter 27 (customs crimes);[34]
- Title 19 of the United States Code, Customs Duties;[35]
- Illegal Exportation of War Materials;[36]
- Search and Forfeiture of Monetary Instruments;[37]
- Passenger Manifests;[38] and
- CBP regulations promulgated pursuant to Titles 8, Aliens and Nationality, and 19, Customs Duties, of the Code of Federal Regulations;[39]
- Section 7208 of The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA);[40]
- Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA);[41]
- Section 205 of the Visa Waiver Permanent (VWP) Program Act of 2000;[42]
- Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act);[43]
- The Implementing Recommendations of the 9/11 Commission Act of 2007;[44]
- Executive Order 13780, Protecting the Nation from Foreign Terrorist Entry into the

[33] 8 U.S.C. §§ 1185, Travel control of citizens and aliens; 1221, Lists of aliens and citizen travelers arriving and departing; 1225, Inspection by immigration officers; and 1357, Powers of immigration officers and employees.
[34] Available at https://www.law.cornell.edu/uscode/text/18/part-I/chapter-27.
[35] 19 U.S.C. §§ 482, Search of vehicles and persons; 507, Officers to make character known; assistance for officers; 1431, Manifests; 1461, Inspection of merchandise and baggage; Examination of baggage; 1499, Examination of merchandise; 1581, Boarding vessels; 1582, Search of persons and baggage; regulations; 1595a, Forfeitures and other penalties; and 1644a, Ports of Entry.
[36] 22 U.S.C. § 401.
[37] 31 U.S.C. § 5317.
[38] 8 U.S.C § 1185(b).
[39] 8 U.S.C. §§ 1185, Travel control of citizens and aliens; 1221, Lists of aliens and citizen passenger travelers arriving and departing; 1225, Inspection by immigration officers; and 1357, Powers of immigration officers and employees.
[40] 49 U.S.C. § 44909
[41] Available at https://www.gpo.gov/fdsys/pkg/CFR-2012-title8-vol1.pdf and https://www.law.cornell.edu/cfr/text/19/chapter-I.
[42] Pub.L. 106-396, 114 Stat. 1637, 1741.
[43] Pub.L. 107-173, 116 Stat. 543, 552.
[44] Pub.L. 110–53.

United States;[45]

- Interim Final Rule on VWP Travelers and 50 Largest Land Ports, August 2004;[46] and
- Final Rule on Additional Alien Categories, December 2008.[47]

## 1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

CBP maintains entry and exit records in accordance with the Border Crossing Information (BCI) SORN.[48] CBP also retains entry and exit records in support of its immigration enforcement mission consistent with the Arrival and Departure Information System (ADIS) SORN.[49] Biometric data stored in the Automated Targeting System (ATS) are covered by their source system SORNs (if applicable) or the ATS SORN,[50] and records associated with a law enforcement action are stored in accordance with the TECS SORN.[51]

## 1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The TVS consists of a group of similar systems and subsystems that support the core functioning and transmission of data between CBP applications and partner interfaces. Due to the similarity in functionality of the biometric cloud matching services used for both entry and exit, this PIA covers both the TVS and TVS-I Systems in a broader context, referring to both systems and their subsystems as the TVS. Under the FISMA, however, both TVS and TVS-I have separate system security plans that have been approved as part of the Certification and Accreditation (C&A) process. The most recent security authorization for the TVS was completed on December 12, 2017, and TVS-I System was completed on April 10, 2018.

## 1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CBP is working with NARA to develop the appropriate retention schedule, based on the new developments described in the Overview. CBP retains photos of in-scope travelers for up to 14 days in ATS-UPAX for confirmation of travelers' identities, evaluation of the technology,

---

[45] 82 FR 13209 (March 6, 2017).
[46] *See* 69 FR 53318 at: http://www.gpo.gov/fdsys/pkg/FR-2004-08-31/pdf/04-19906.pdf.
[47] *See* 73 FR 77473 at: http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/pdf/E8-30095.pdf.
[48] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[49] *See* DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2015).
[50] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[51] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

assurance of accuracy of the algorithms, and system audits. In addition, CBP is sharing the facial images of in-scope travelers with IDENT to allow for more accurate future matching against newly-captured photos. The retention of these photos in IDENT will follow DHS Office of Biometric Identity Management's (OBIM) IDENT retention schedule.[52] However, CBP does not retain or share facial images of U.S. citizens, nor does it store the images in IDENT or any other CBP or DHS database. Finally, CBP promptly discards all photos, regardless of immigration or citizenship status, from the TVS cloud matching service.[53]

### 1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information maintained within the TVS, with the exception of law enforcement information, is covered by the PRA. OMB 1651-0138, Agency Information Collection Activities: Biometric Identity expires on July 31, 2019.

## Section 2.0 Characterization of the Information

### 2.1 Identify the information the project collects, uses, disseminates, or maintains.

In order to properly evaluate travelers at the border, CBP collects specified biographic and travel information[54] and conducts pre-arrival or pre-departure TECS queries. CBP uses this information to conduct checks against lookouts, such as wants and warrants, watch list matches, etc., entered by law enforcement officers or received from the ATS and confirmed by a CBPO based on threshold targeting rules. For travelers at air and sea ports of entry, CBP collects personal information from the APIS manifest. This manifest typically includes the following data elements: name; date of birth; country of citizenship; passport information (number, country of issuance and expiration date); and travel itinerary information (i.e., for air travelers, flight number, carrier, originating, and destination airports).

Based on the list of confirmed travelers, often in the APIS manifest, the TVS collects facial images from travelers. For technical demonstrations at the land border, air entry, and some air exit operations, CBP captures the images of travelers on CBP-owned cameras. In other air exit and seaport demonstrations, CBP works with specified partners, such as commercial air carriers,

---

[52] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.
[53] Photos of all travelers, including U.S. citizens, are held in the secure TVS cloud matching service for no more than 12 hours after identity verification, in case of an extended system outage.
[54] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (December 22, 2010), *available at* www.dhs.gov/privacy.

airport authorities, and cruise lines, which 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 identity verification.

Please see the Appendices to a detailed description of the various methods of collection.

## 2.2 What are the sources of the information and how is the information collected for the project?

Biometric data located in the TVS is collected directly from the members of the traveling public. Information is obtained directly from travelers, or from the travelers via the commercial carrier, prior to entry to and departure from the United States. In addition, CBP retrieves the historical photos, which are matched against the newly-captured photos, from the Department of State (DoS) and other DHS holdings such as IDENT. The U.S. Government collected these historical images directly from the individuals, such as when the travelers obtained their passports, applied for a visa, or crossed the border in the past.

## 2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. The TVS does not receive direct feeds of information from commercial data aggregators, and it does not collect data from public sources.

## 2.4 Discuss how accuracy of the data is ensured.

CBP uses the facial images collected in the TVS to continually test and evaluate the accuracy of the camera technology and the algorithms. CBP retains the images of in-scope travelers for up to 14 days in order confirm travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. However, CBP does not retain images of U.S. citizens once their identities have been verified.[55] CBP staff manually review system-generated matches related to the identification of a U.S. citizen in order to confirm that the match has been generated correctly. Airlines, airport authorities, and cruise line companies that deploy their own camera operators and camera technology must meet CBP's technical specifications and security requirements in order to connect with CBP's TVS and use the matching service.[56] Each camera must be linked to the TVS via a secure, encrypted connection, and the biometric data must

[55] Photos of all travelers, including U.S. citizens, are held in secure CBP systems for no more than 12 hours after identity verification, in case of an extended system outage.

[56] CBP requires facial images captured at the departure gate to conform closely to the International Civil Aviation Organization (ICAO) standards (ISO 19794-5) 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.

be encrypted both at rest and in transit. In addition, 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 analyzing the performance of algorithms as a true positive rate, false positive rate, false match rate, and false non-match rate. CBP is also collaborating with S&T, OBIM, and the National Institute of Standards and Technology (NIST) to test technologies developed by specified vendors and to evaluate algorithms on biometric projects.

### 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a risk that the facial images collected through the TVS process will not be of high enough quality or be an accurate representation of the traveler, therefore negatively impacting the reliability of the matching service.

**Mitigation:** This risk is mitigated. CBP is fully committed to testing new processes and capabilities for using facial recognition technology to verify the entry and departure of travelers to the United States. To do so, CBP must balance the practical challenges of processing a large volume of travelers in a short period of time and minimal infrastructure for outbound travelers, with the mandate to implement a comprehensive biometric entry/exit program. After extensive research, CBP has found facial recognition to be the most efficient, effective, accurate, and less invasive biometric approach.

CBP is continually testing and evaluating the accuracy of the camera technology and the algorithms. Prior to deploying any modification to the technology or the process (e.g., the Vehicle Face technical demonstration discussed in Appendix A), CBP conducts tests to assess impacts to the traveler and the accuracy of the information to ensure there are no adverse impacts. These tests are for assessment purposes only, and data collected during this process is not used operationally. CBP maintains the photos of in-scope travelers for up to 14 days to aid in confirming the travelers' identities, evaluating the technology, ensuring the accuracy of the algorithms, and facilitating system audits. Additionally, DHS S&T tests the effectiveness of commercial, academic, and government algorithms in matching facial images. S&T identifies how each algorithm performed as a true positive rate, false positive rate, false match rate, and false non-match rate. CBP is also partnering with S&T, OBIM, and NIST to evaluate algorithms and test biometric technologies developed by specified vendors.

## Section 3.0 Uses of the Information

### 3.1 Describe how and why the project uses the information.

CBP will use the information it collects through its own TVS camera technology, as well as through its public and private sector partners, to verify traveler identities and create entry and 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; in addition, photos of in-scope travelers stored in IDENT are available to approved users consistent with the terms for existing traveler biometric records. CBP generates entry and exit records primarily in support of its mission to facilitate legitimate travel and enforce immigration laws, such as via counterterrorism and immigration enforcement activities.

CBP business partners, including airlines, airport authorities, and cruise lines, may take photos of travelers and share them with the TVS through an authorized integration platform or other vendor. CBP's business requirements do not permit its partners to retain or share the photos captured at the boarding gate for the purposes of identity verification through the TVS. CBP briefly maintains the facial image templates in the TVS for the purpose of identity verification by matching travelers with templates of historical photos. CBP's ATS-UPAX discards photos of all travelers within 14 days but does not retain photos of U.S. citizens for any length of time. Additionally. the TVS cloud matching service does not retain any traveler photos.[57] CBP may 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.

### 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. The TVS system does not conduct electronic searches, queries or analyses in search of predictive patterns or anomalies, nor does CBP use the facial images captured through this process for such activities.

### 3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. CBP is partnering with TSA to test the capturing and matching of facial images at the TSA checkpoint. TSOs view some biographical information for each traveler, as well as the results of the match. Additionally, CBP's TVS shares pictures of in-scope travelers with DHS OBIM's IDENT System for secure storage.

### 3.4 Privacy Impact Analysis: Related to the Uses of Information

**Privacy Risk:** There is a risk that CBP will use exit records created under the TVS for a

[57] Photos of all travelers, including U.S. citizens, are held in the TVS cloud matching service for no more than 12 hours after identity verification, in case of an extended system outage.

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 may 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:** Because the TVS uses facial images from a variety of sources, both public and private, there is a risk that the airline, airport, and cruise line partners will use the biometric data for commercial or marketing purposes, or for a purpose other than identity verification.

**Mitigation:** This risk is partially mitigated. CBP partners such as select air carriers, airport authorities, and cruise lines may capture photos of travelers and share them with the TVS via an authorized integration platform or other vendor. CBP stores the images, in the form of irreversible photo templates, in the TVS cloud for the purpose of matching travelers with previous photos and thus verifying their identities. ATS-UPAX deletes photos of all travelers within 14 days but does not retain the photos of U.S. citizens. The TVS cloud matching service retains photos of all travelers for no more than 12 hours.

Only authorized representatives of the approved partners may obtain access to the collection device. The business requirements implemented by CBP with its partners govern the retention and use of the facial images collected under the TVS. CBP does not permit its approved partners to retain the images, which are being collected for the purposes of identity verification through the TVS, for longer than is necessary in order to achieve the intended purpose of the original collection. Finally, CBP requires its partners to encrypt the biometric data, both at rest and in transit.[58] 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.

[58] Under the TVS-partners initiative, industry partners may collect separate photographs consistent with their contractual relationships with the travelers, rather than under CBP authorities, for commercial purposes. This collection is subject to the contract between the industry partner and the traveler, to which CBP is not a party. CBP cannot limit the use of the biometric information that is collected separately by a business partner for its own business purposes. In line with these business requirements, as of the date of this PIA, no air exit partner had communicated to CBP any plans to collect separate images at the departure gate for its own purposes.

# Section 4.0 Notice

## 4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

As CBP continues to expand upon its biometric entry and exit operations through use of the TVS, CBP will continue to provide notice to travelers at the designated ports of entry through both physical and either LED message boards or electronic signs as well as verbal announcements in some cases to inform the public that CBP will be capturing the photos for identity verification purposes, and that U.S. citizens may currently request alternative processing from a CBPO, should they wish to opt-out of the biometric process. In addition, CBP's public notices notify travelers that CBP will retain the photos in secure DHS IT systems, with the exception of photos of U.S. citizens, which are not retained unless linked to an enforcement record. These notices will direct travelers who have questions to the CBP Info Center. When CBP operates TVS in conjunction with approved partner organizations, the public is informed that the partner is collecting the biometric data in coordination with CBP.

Upon request, CBPOs provide individuals with a tear sheet with Frequently Asked Questions (FAQ), opt-out procedures, and additional information on the particular demonstration or program, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information. Additionally, in the Federal Inspection Services (FIS), CBP posts signs informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States. TSA posts visible signs at the TSA airport checkpoint describing the partnership with CBP, along with procedures relating to the aforementioned technical demonstration. Information on CBP biometric entry and exit projects is also available on the official CBP public website. CBP issues press releases and updates to its website as it deploys new biometric exit processes at new locations and through different modalities. CBP provides additional notice to the public through this PIA and will publish updates or additional PIAs relating to future changes.

## 4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Generally, there is no opportunity for an individual to decline to provide information that is required in order to travel to or from the United States. Pursuant to CBP's border search and immigration authority, an individual seeking entry into the United States must satisfy the CBPO that he or she is a U.S. citizen, lawful permanent resident, or is otherwise eligible for admission to the United States, and that he or she is not attempting to import or export any merchandise in violation of U.S. laws. Similarly, individuals departing the United States may be subject to CBP inspection to support the creation of exit records and as required for law enforcement operations.

However, U.S. citizens who do not wish to provide a facial image to CBP may opt out of this requirement and request alternative processing by seeing a CBPO. For the CBP-TSA technical demonstration, TSA and CBP allow travelers to decline to participate and proceed with normal TSA processing.

## 4.3 Privacy Impact Analysis: Related to Notice

**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, individuals seeking to travel internationally are subject to the laws and regulations enforced by CBP and are subject to inspection. If a U.S. citizen requests not to participate in the TVS, an available CBP Officer may use manual processing to verify the individual's identity. Additionally, 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 Traveler Redress Inquiry Program (TRIP).[59] 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.

**Privacy Risk:** There is a risk that the individual may not know that his or her information is being collected and retained by CBP, particularly if the collections are operated by a commercial carrier, other government agency, or international partner.

**Mitigation:** This risk is mitigated through multiple avenues of public notice. CBP uses verbal announcements and signage, both physical and electronic, in order to inform the traveling public of CBP's intent to capture facial images for the purposes of verifying the identity of travelers and maintaining the images of in-scope travelers in secure DHS systems. Whenever possible, CBP posts the signage in areas that provide travelers with enough notice of the collection to enable them to approach a CBPO for additional information. Additionally, TSA posts signs at the TSA airport checkpoint explaining the partnership with CBP, as well as procedures for either participating in the technical demonstration or requesting alternative processing. For the vehicle at speed process, it is more challenging to ensure that drivers view the signs and are aware of the capture of their facial image; to address this issue, CBP provides both electronic and physical signs in visible locations prior to the port of entry's vehicle infrastructure, as well as signs in each vehicle lane. CBP also provides tear sheets with additional details and FAQs, upon request, and may direct travelers to the CBP Info Center, should they have questions. Finally, CBP's public website, as well as this PIA and press releases, as demonstrations are announced, provide further notice of this

[59] DHS/ALL/PIA-002 DHS Traveler Redress Inquiry Program (TRIP), *available at* www.dhs.gov/privacy.

collection. CBP's various notices inform U.S. citizens that they may ask a CBPO for an opportunity for alternative processing, and that their photos will not be retained. For technical demonstrations operated by both CBP and an approved partner organization, CBP and the partner collaboratively develop plans for informing the public of the partner's collection of the photos on behalf of CBP and coordinate to ensure that signs are posted, tear sheets are available, and additional information is posted on the CBP website and in press releases.

# Section 5.0 Data Retention by the project

## 5.1 Explain how long and for what reason the information is retained.

CBP retains biographic exit records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens, consistent with the BCI SORN.[60] Records associated with a law enforcement action are retained for 75 years in accordance with the TECS SORN.[61] CBP retains biographic entry and exit records in ADIS[62] for lawful permanent residents and non-immigrant aliens, consistent with the SORN.

As CBP verifies the identity of the traveler, either through the automated TVS facial recognition process or manual officer processing, the backend matching service returns the "match/no-match" result, along with the respective associated UID, to ATS-UPAX. CBP temporarily retains facial images of non-immigrant aliens and lawful permanent residents for no more than 14 days within ATS-UPAX for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. CBP does not retain photos of U.S. citizens, once their identities have been confirmed.[63] Photos of all travelers are purged from the TVS cloud matching service within a brief number of hours, depending on the mode of travel. Photos of in-scope travelers are retained in IDENT for up to 75 years, consistent with existing CBP records that are housed in IDENT in accordance with the BCI SORN.

## 5.2 Privacy Impact Analysis: Related to Retention

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

**Mitigation:** This risk is mitigated. CBP does not retain facial images of U.S. citizens once their identities have been verified, in ATS-UPAX or the TVS cloud matching service.[64] CBP

[60] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[61] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[62] *See* DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* www.dhs.gov/privacy.
[63] CBP retains photos of U.S. citizens in secure CBP systems only up to 12 hours after identity verification, in case of an extended system outage.
[64] The TVS cloud retains photos of all travelers, including U.S. citizens, for up to 12 hours after identity verification, in case of an extended system outage.

maintains biographical information on U.S. citizens for no more than 15 years, consistent with existing policies, in accordance with the BCI SORN.

**Privacy Risk:** There is a risk that a partner airline, airport authority, or cruise line will retain biometric information longer than is necessary.

**Mitigation:** This risk is partially mitigated. CBP's business requirements for its partners, along with this PIA, govern partner retention practices. CBP requires its partners to delete the TVS photos following transmission to the TVS. While an approved partner may collect photos of travelers using its own equipment under its own separate business process for commercial purposes, as of the publication of this PIA, no such partner had communicated to CBP any plans to do so.

# Section 6.0 Information Sharing

## 6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBP will continue to share biographic entry and exit data, consistent with the terms described in the relevant SORNs listed above in Section 1.2. 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 updates its notices for any new uses. Consistent with existing practice, CBP entry and exit records for non-U.S. citizens are available to authorized users of IDENT who may access this data in support of their own law enforcement missions.[65]

Under the TSA exit demonstration and the partner process initiative, CBP may share the result of the TVS match (i.e., simply a "match" or "no match" result) with the approved partner agency or organization in order to allow the traveler to proceed. For instance, in air exit, the TVS provides a "green light" for the partner airline or TSO to permit the traveler to continue through the screening process. Similarly, the TVS provides a "green light" for the partner airline to permit the traveler to depart the United States and board the aircraft. In the case of a negative result, the TSO or partner organization would either adjudicate the "no match" and/or direct the traveler to a CBPO. This limited sharing of information will be covered by business requirements that CBP is developing for its partner organizations.

CBP shares the facial images of in-scope travelers within DHS, with IDENT, and on occasion with S&T for testing purposes. CBP also partners with NIST to test technologies developed by specified vendors and to evaluate algorithms on biometric projects. However, CBP

[65] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.

does not share U.S citizens' biometric data from the TVS with any other external federal entity. If external sharing became necessary, CBP would develop business requirements, an MOU, and/or Information Sharing Agreement (ISA) to cover any interface implemented between CBP and an outside entity to specify the general terms and conditions to govern the use of the functionality or data, including types of information and privacy-related limitations on use.

### 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing of the TVS match/no match results with approved partners outside the Department is compatible with the identity verification purposes for which the information in the TVS is collected as well as business requirements CBP develops for its approved external partners. In addition, the sharing of the facial images of non-U.S. citizens with IDENT is compatible with the applicable SORNs. If additional external sharing becomes necessary, CBP will develop business requirements, an MOU, and/or ISA to cover any interface implemented between CBP and an outside entity, such as NIST and the airline, airport, or cruise partners, to specify the general terms and conditions that would govern the use of the functionality or data, including types of information and privacy-related limitations on use.

### 6.3 Does the project place limitations on re-dissemination?

Yes. CBP shares information only pursuant to routine uses outlined in the SORNs listed above under Section 6.2 above or through business requirements, an approved MOU, or ISA, such as the sharing described in Section 6.1. In addition, CBP re-disseminates information only in accordance with the Privacy Act.

### 6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Requests for records from the TVS should be made to the Executive Assistant Commissioner, Office of Field Operations and the Director, Targeting and Analysis, Systems Program Office, Office of Information and Technology, U.S. Customs and Border Protection, both of which are located at 1300 Pennsylvania Avenue N.W., Washington, D.C. 20229. All such requests must be reviewed and approved by the CBP Privacy Office and are documented using DHS Form 191.

### 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a risk to information sharing that a commercial partner will improperly share the facial images or results of the TVS match with a third party.

**Mitigation:** This risk is partially mitigated. While CBP enters into arrangements with commercial partners that communicate the terms of the information sharing under the TVS partner process, CBP does not govern how commercial partners use biometric data that they collect

separately pursuant to their own agreements with their customers. CBP is developing business requirements with its airline, airport authority, and cruise line partners that will specify that the partners must immediately delete the photos, captured for the purpose of identity verification through the TVS, as soon as the photos are transmitted to the TVS. In addition, any associated partner IT system must provide a method for CBP to audit compliance with this requirement.

# Section 7.0 Redress

## 7.1 What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to biometric information contained in the TVS, or seeking to contest the results of the biometric matching process may gain access to certain information in the TVS by filing a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229
Fax Number: (202) 325-1476

All Privacy Act and 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. Requests for information are evaluated by CBP 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.

## 7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The biometric information within the TVS is part of the BCI System of Records. Biometric data is also stored within the ATS System of Records. CBP maintains entry and exit records on lawful permanent residents and non-immigrant aliens in the ADIS System of Records. Finally, records associated with a law enforcement action are part of the TECS System of Records. Individuals may access their information via a Privacy Act or FOIA request to the DHS Chief FOIA Officer or the CBP FOIA Officer.

If a traveler believes that CBP actions are the result of the TVS maintaining incorrect or inaccurate information, (i.e., if the TVS finds a mismatch, false match, or "no match") inquiries may be directed to:

U.S. Customs and Border Protection

CBP Info Center
Office of Public Affairs
1300 Pennsylvania Avenue
Washington, DC 20229

Travelers may also contact the DHS Traveler Redress Inquiry Program (DHS TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/dhs-trip if they have experienced a travel-related screening difficulty, including those they believe may be related to incorrect or inaccurate biometric information retained in their record(s). Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

## 7.3 How does the project notify individuals about the procedures for correcting their information?

The TVS contains travelers' facial images, which CBP uses for identity verification. CBP has designed the entry and exit inspection process such that, if a mismatch, false match, or "no match" is found, CBP may use alternative means to verify the traveler's identity and ensure that he or she is not unduly delayed. In the event that an individual does experience a delay or issue as an outcome of these processes, travelers are informed of the avenues for redress in Section 7.2 of this PIA. Signage and tear sheets at select ports of entry where the TVS is employed provides information on how to contact the CBP Info Center and/or DHS TRIP. In addition, travelers may request information from the on-site CBPO.

## 7.4 Privacy Impact Analysis: Related to Redress

**Privacy Risk:** There is a risk that individuals may not know how to request redress relating to accessing their records.

**Mitigation:** This risk is mitigated. CBP has described redress procedures in this PIA as well as relevant system SORNs. CBP and DHS provide notice to the public of their redress rights on their websites. In addition, CBPOs, along with tear sheets if requested, direct travelers to the CBP Info Center and DHS TRIP to learn about additional opportunities for redress. The process has not changed and the CBPO continues to verify any abnormalities, law enforcement concerns, fraud or imposters concerns, etc. in the same manner as before. CBP could send a request to OBIM's Biometric Support Center to disassociate incorrect biometrics and biographic information and re-enroll the biometrics to the correct biographic information should that issue arise.

**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 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. 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, lawful permanent residents, or 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 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.

# Section 8.0 Auditing and Accountability

## 8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CBP access controls ensure only authorized access to the facial image data. The facial image data cannot be accessed or released for any unauthorized use. The photos collected cannot be viewed at the collection location (departure loading bridge) or at the time of collection. CBP 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 (meaning if an unauthorized user were to view the template, it would not be visible as a facial image). CBP stores TVS information in secure CBP systems and temporarily in a secure virtual cloud environment. CBP uses two-factor authentication and strong encryption to transfer the data between the camera, the TVS cloud matching service, and CBP systems as well as for PII at rest. In accordance with DHS IT Security procedures, TSA also provides similar authentication for its TSOs who use the mobile device, in addition to strong encryption of traveler data, both at rest on the device and in transit between the device and CBP's TVS.

CBP does not retain photos of U.S. citizens in any IT system. No photos are retained on any travelers in CBP systems for more than 14 days, but photos of in-scope travelers are shared with IDENT. CBP partners may sometimes capture photos of travelers, store them using their own IT infrastructure, and use them for their own business purposes, separately from the TVS process. However, CBP's business requirements do not permit its partners to store the photos, captured for the purpose of TVS matching and identity verification process, for longer than the minimum

amount of time necessary to transmit the photos to the TVS. Additionally, the CBP partner's IT system must provide access for CBP to audit compliance with this retention requirement. Moreover, just as CBP encrypts all biometric data at rest and in transit, CBP requires its approved partners under the TVS partner process to encrypt the data, both at rest and in transit. CBP will document the deletion of data from UPAX and the encryption keys for the cloud service provider are stored using the provider's Key Management Service, on hardware hosted by the provider. 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 cloud service provider's auditing services allow the TVS to monitor every time the key is accessed programmatically.

The cloud service provider selected for this initiative is required to adhere to the security and privacy controls required by NIST Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing,"[66] and the DHS Chief Information Officer.

The CBP Privacy Office will conduct a CBP Privacy Evaluation 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. The results of the CBP Privacy Evaluation will be shared with the DHS Privacy Office.

## 8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Initial TVS access is not activated for an individual without completion of the CBP Security and Privacy Awareness course. The course presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official information and PII. The course also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and TVS users are required to take the course annually.

## 8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

All access procedures ensure that the roles for all TVS users have the valid access authorization, based on the specified role and the "need to know." TVS assigns non-privileged accounts to end users and privileged accounts to account managers or administrators in order to manage and maintain the application. Both types of accounts ascribe profiles for role-based access control. The TVS system owner determines the conditions for role membership and designates selected individuals to serve as account managers for the system. Once a user successfully completes the application for a TVS account, his or her supervisor identifies which TVS system

[66] *See* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

role(s) are needed to accomplish the job, and the account manager determines account access. Users who wish to view a project are required to request approval from that project's access manager, who assigns roles. The TVS Information System Security Officer (ISSO) tracks and review all user actions on a monthly basis. Before a user is assigned a role-based account, CBP requires the user to pass a full CBP Background Investigation, complete the CBP Security and Privacy Awareness Training, and demonstrate a valid business need. These roles can be removed and modified at any time with consent of the project's access management. For CBP's TVS partner process, only authorized representatives of approved CBP partners have access to the collection device, i.e., the camera technologies.

All TVS accounts are continuously monitored by the system administrator and are reviewed annually by each user's supervisor to ensure that there is still a need to know, based on the user's role. Regular reviews ensure that the users are compliant, based on their roles and activities and in accordance with DHS policy. Accounts are automatically disabled after 30 days of inactivity and are removed after the user's supervisor submits an employee separation form. All of the processes described above are automated, based on either scripts or notifications via email.

### 8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All business requirements, MOUs, and ISAs are reviewed by the respective CBP program manager within the CBP Office of Field Operations, in consultation with the Office of Information Technology. Agreements involving PII are also generally approved by the CBP Privacy Officer, the Office of Chief Counsel, and DHS in accordance with procedures developed by the DHS Information Sharing Governance Board.

## 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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

# Appendix A: CBP Owned and Operated Camera Collection Sites

*Last Updated: November 14, 2018*

## 1. Air Entry/Simplified Arrival

TVS deployment for processing arriving air travelers mirrors the process for air exit, with manifest-based galleries and a similar facial recognition algorithm, but integrates it into CBP's entry inspection applications. Historically, prior to admission to the United States, CBP has used a manual process to inspect travel documents such as passports or visas in order to initiate system checks and verify a traveler's identity, travel history, and any law or border enforcement concerns that may require attention. The new primary entry solution uses biometrics to initiate the transaction and system checks, using facial recognition as the primary biometric verification modality. This shift from a biographic, document-based system to biometrically initiated transactions requires travelers to provide facial photos for identity verification purposes.

In 2017, CBP deployed Simplified Arrival, the new biometric primary entry process, at one airport, and a number of airports and airlines have followed suit. CBP uses commercial off-the-shelf cameras, CBP's primary arrival subsystem of TECS,[67] and the TVS to capture facial biometric data from travelers seeking to enter the United States. Under this new automated entry process, CBP obtains biographic information from the APIS manifest on travelers boarding international flights. The airline-generated UID is attached to the manifest but is not specifically used during Simplified Arrival. CBP screens the APIS information against TECS records and other law enforcement databases in order for CBP to ascertain if any security or law enforcement risks exist. For Simplified Arrival, all travelers proceed to the entry lanes within CBP's FIS, where a camera captures an image of the traveler's face. The TECS primary arrival subsystem transmits the image to the TVS. In order to biometrically identify the traveler, the TVS automatically creates a template from the image and uses the template to query against a gallery of known identities, based on the manifests for all incoming flights for that day.

Once the traveler is matched, the TVS transmits the match results, along with a TECS system-generated unique traveler identifier and an ATS-UPAX-generated unique photo identifier, to TECS. In turn, the TECS primary arrival subsystem uses the TECS-generated identifier to retrieve the traveler's biographic information from the APIS manifest. Additionally, the TECS subsystem uses the ATS-UPAX-generated identifier to retrieve the historical image (which had matched with the new image) stored in UPAX. The CBPO has the ability to view and evaluate the traveler's biographic data, along with any derogatory information, in the TECS primary arrival application, along with associated biometric match results from the TVS. The CBPO then conducts the standard inspection interview and establishes the purpose and intent of travel. Once CBP

[67] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (December 22, 2010), *available at* www.dhs.gov/privacy.

determines admissibility, the CBPO either refers the traveler to secondary processing for further inspection or directs the traveler to baggage claim. In general, this automated process eliminates the need for the CBPO to scan the individual's travel documents, unless a particular concern arises.

Upon admission, CBP updates the traveler crossing history in TECS to reflect a confirmed arrival into the United States. Consistent with the existing process for non-U.S. citizens, CBP updates the crossing history with OBIM's IDENT to reflect a biometrically confirmed arrival into the United States. Alternatively, if the TVS matching service determines that a particular traveler is a U.S. citizen, CBP bypasses photo storage of that encounter, and the photo is not retained.[68] However, if the traveler presents himself or herself as a citizen of another country, CBP processes and retains the photo accordingly.[69]

CBP continues to assess additional process improvements related to air entry, including the use of the TVS facial recognition solutions at Global Entry[70] as well as in support of preclearance processes.[71] The list of airports where Air Entry/Simplified Arrival is deployed is available at https://www.cbp.gov/travel/biometrics (see "Experience it Here").

## 2. Air Exit

When 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 TVS cloud matching service via a secure, encrypted connection. Once the camera captures a quality image and the system successfully matches it with a photo template from the gallery associated with the manifest, the traveler proceeds to board the plane.

If the image created by the facial recognition camera system does not match the photograph template on file associated with the individual's travel document, the operator directs the traveler to a CBPO stationed at the passenger loading bridge. The CBPO uses the wireless BE-Mobile handheld device[72] to verify the traveler's identity using either fingerprints for aliens, via a query in the OBIM IDENT, or by conducting an inspection to ensure the traveler is holding valid travel documents. If the CBPO is unable to locate a record of the traveler's fingerprints in IDENT, the

[68] Photos of all travelers, including U.S. citizens, are held in secure CBP systems for no more than 12 hours after identity verification, in case of an extended system outage.
[69] For example, a U.S. citizen who is also a citizen of another country and traveling on a foreign passport would be processed as a foreign national until CBP can verify his or her status as a U.S. citizen.
[70] *See* DHS/CBP/PIA-002 Global Enrollment System (GES): Trusted Traveler Program System (August 15, 2017), *available at* www.dhs.gov/privacy. CBP will describe the use of facial recognition at Global Entry kiosks in a forthcoming update to the GES PIA.
[71] CBP Preclearance provides for the U.S. border inspection and clearance of commercial air passengers and their goods in certain foreign countries. A preclearance inspection is essentially the same inspection an individual would undergo at a U.S. port of entry. Visit https://www.cbp.gov/border-security/ports-entry/operations/preclearance for a list of CBP preclearance locations.
[72] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Program (July 5, 2018), *available at* https://www.dhs.gov/privacy.

officer may run a separate criminal history check in the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) Integrated Automated Fingerprint Identification System (IAFIS),[73] and enrolls the fingerprints in IDENT. The list of airports where Air Exit is deployed is available at https://www.cbp.gov/travel/biometrics (see "Experience it Here").

### 3. Land Entry

Travelers may transit the U.S. land border in a commercial or personally-owned vehicle, or as pedestrians. At entry and departure points of select ports along the Southwest land border, CBP is testing facial recognition technology to capture the photos of pedestrian crossers and vehicle occupants. This process supports CBPOs in the potential detection of imposters arriving at the border by verifying the validity of travel documents and verifying the identities of travelers. Unlike in the air and sea environments, although CBP does receive voluntary manifests from private rail and bus lines,[74] there are no manifests for pedestrians crossing the land border on foot or in personal vehicles to support creating a gallery of known travelers. CBP is developing processes that would enable the use of TVS at the land border; for example, CBP may briefly retain local galleries of travelers who have recently crossed at a given Port of Entry and are expected to cross again within a given period of time.

In order to facilitate and expedite vehicle crossings at the land border, CBP is testing several biometric technologies. The Vehicle Face demonstration uses facial recognition devices at vehicle inbound and outbound lanes in order to capture the facial images of vehicle occupants "at speed" (under 20 mph) and biometrically match the new images against a TVS gallery of recent travelers. CBP has created a discrete, non-production instance of the TVS for this demonstration, separate from the current TVS cloud-based matching service used for Air Entry (i.e., Simplified Arrival) and Air Exit. CBP has installed several cameras in inbound lanes just prior to the existing vehicle lane infrastructure and in outbound lanes just beyond the license plate reader vehicle footprint. Vehicles proceed through the respective inbound and outbound lanes as normal, with Officers processing vehicle occupants at the primary inbound booths using existing CBP software applications and technology.

This process captures the biographic data of the vehicle occupants, associates the travelers with the vehicle, and creates an exit crossing record for the occupants.[75] The identification numbers assigned to the exit crossing records are associated with scene and facial images captured during this demonstration so that analysts can later compare the biographic crossing data with the facial

---

[73] *See* Privacy Impact Assessment: Integrated Automated Fingerprint Identification System National Security Enhancements, *available at* https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis.
[74] *See* DHS/CBP/PIA-001(d) Advanced Passenger Information System-Voluntary Rail and Bus Submissions (February 19, 2009), *available at* www.dhs.gov/privacy.
[75] *See* DHS/CBP/PIA-009 TECS System – Primary and Secondary Processing (December 22, 2010), *available at* www.dhs.gov/privacy.

images and biometric matching. CBP is not retaining photos of U.S. citizens and is not sharing with IDENT but is storing the facial images of foreign nationals collected during this demonstration in an offline, non-production TVS database located on the CBP network until December 2020 for the purpose of analysis and evaluation. Initially, this demonstration will not impact the current experience of the travelers or officers, except during normal outbound "pulse-and-surge" operations in which CBPOs stop vehicles and process the occupants using a TECS System application.

CBP is testing the use of biometric camera technology to verify the identities of drivers and passengers of commercially-owned vehicles (COV) entering the United States at speeds less than 10 miles per hour. Similar to the air environment, COVs are required to submit a manifest to CBP before arriving at a port. In addition to cargo information, these manifests include the names of drivers and any passengers. CBP will use these names to retrieve historical photos from the TECS Travel Document Encounter Database subsystem and to populate the TVS gallery. As they approach the border in the COV, cameras owned by port operators will capture facial images from the drivers and passengers in order to compare the images with the historical photos from the manifest using the TVS.[76] These pictures are not accessible by port operators and are sent via secure connection to a computer in the CBP booth. If the match is positive, the TVS notifies the CBPO in the booth, who will determine if any further inspection is necessary before permitting the COV to cross the border and enter the United States. If the matching process results in a "no match," the CBPO will stop the COV at the inspection booth for further processing. These images will only remain in the TVS for up to 24 hours, and CBP will not retain any facial images captured during the crossing. The list of land ports of entry where TVS is deployed is available at https://www.cbp.gov/travel/biometrics (see "Experience it Here").

## 4. Land Exit

In addition to demonstrating the value of the use of facial recognition on entry, CBP is also determining the feasibility of capturing the photos of all departing pedestrians, using TVS cameras with a Radio Frequency Identification (RFID) document reader positioned in the outbound pedestrian crossing area. Travelers with an RFID travel document approach the camera, place the document near the reader, and the document retrieves the traveler's biographic information. After a facial image is captured and a template is created, the TVS performs a match of that template to the gallery of recent crossers generated during the entry process. For travelers without an RFID document, the camera captures their photos and sends them to the TVS for comparisons against the gallery of recent crossers. Following the match, in a manner similar to the entry operations described above, TECS uses the biographic data to perform law enforcement queries, the results of which TECS displays to the CBPO, along with the newly-captured image and the matched

[76] *See* DHS/CBP/PIA-021 TECS System: Platform (August 12, 2016), *available at* www.dhs.gov/privacy.

photo. For positive matches, travelers are allowed to proceed, and the crossing history is updated in TECS and ADIS to reflect a biometrically confirmed departure from the United States. As travelers depart, CBPOs who operate under a "pulse and surge" approach[77] may use the BE-Mobile[78] device to view non-matches and derogatory biographic information.

CBP has begun recording the final departures of Third Country Nationals (TCN) encountered during outbound operations at land crossings, both biographically and with facial images and fingerprint biometrics. A TCN is defined as a foreign national who is attempting to enter either Canada or Mexico but is not a citizen of either country. TCNs departing the U.S. by land are those individuals who are currently subject to biometric collection under existing CBP regulations.[79] CBP uses a "pulse and surge" strategy to inspect people, cargo, and conveyances leaving the United States at all airports, seaports, and land border crossings. CBP is conducting outbound operations, both intelligence-based and on a random basis using the BE-Mobile device.[80] Initially, CBP is testing the process at several locations; once tested and evaluated, CBP plans to deploy this strategy nationally. The list of land ports of entry where TVS is deployed is available at https://www.cbp.gov/travel/biometrics (see "Experience it Here").

## 5. Seaport Entry

Inbound and outbound processing for travelers on commercial sea vessels (e.g., cruise ships) will resemble the air entry and exit processes, as this travel method is also based on a passenger manifest. Traditionally, for vetting purposes, cruise lines have submitted biographic and travel document information to the U.S. Coast Guard's (USCG) electronic Notice of Arrival and Departure (eNOAD)[81] System. USCG routed this information to CBP's APIS approximately 60 minutes in advance of departure from and up to 96 hours prior to the arrival of a cruise line in the United States. Because the timing of the data transmission impaired CBP's ability to effectively vet cruise passengers and allow sufficient time for more sophisticated data analysis, such as the application of rules or algorithms, CBP is reengineering this process.

The new process will facilitate the transmission of reservation data directly from the cruise lines to CBP three days in advance of embarkation. The direct submission of the manifest to CBP will allow for more flexible time tables and will also include additional reservation-related data elements and facial images for matching purposes. Cruise lines will continue to submit the passenger information to USCG's eNOAD but will make an additional submission to CBP through secure web services. In turn, the router will send the following data transmissions: (1) the

---

[77] Pulse and surge operations are short-term enforcement operations that increase the frequency of outbound inspections at specific ports, either randomly or based on intelligence.
[78] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (June 18, 2015), *available at* www.dhs.gov/privacy.
[79] 8 CFR Part 215.
[80] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (June 18, 2015), *available at* www.dhs.gov/privacy.
[81] *See* DHS/USCG/PIA-006 Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System (AIS), *available at* www.dhs.gov/privacy.

biographic and travel document information directly to APIS; and (2) the Passenger Name Record (PNR) data and facial images of the travelers, if available, to the ATS-UPAX.

CBP has also begun building partnerships with the cruise line industry in an effort to use facial recognition technologies to improve security and enhance the efficiency of inspections in the cruise environment. Under the Simplified Arrival - Seaport process, CBP again uses a gallery of historical photos from DHS holdings in the TVS gallery for the purpose of matching these previous photos with a newly-captured photo. CBP is using TVS to build a gallery, based on the APIS manifest, of traveler photographs using a gallery of photos from DHS holdings to be compared to newly-captured photographs. Once the vessel arrives at the U.S. Port of Entry, cruise lines employ cameras to collect facial photographs of passengers as they debark. The cruise lines submit the facial image to the TVS, which creates a template of the photo and performs the facial matching. If the matching process returns a positive result, CBP will indicate to cruise personnel that CBP has verified the traveler's identity. Travelers for whom the matching process returns a negative result will be directed to a CBPO for inspection. Travelers who are U.S. citizens may choose to inform the cruise line that they do not wish to participate in the photo collection process by opting-out, but will instead submit to a CBPO's inspection. Once CBP allows the traveler to proceed, the traveler advances to the baggage area and to egress through the FIS. CBPOs operate in a roving enforcement capacity within the terminal facility and FIS. Subsequent phases of the Simplified Arrival-Seaport technical demonstrations will likely add the capture of travelers' photos and matching with historical photos at a cruise's embarkation (exit) point, in addition to the use of the TVS at debarkation. In a future phase, CBP will also receive the facial images captured by the cruise line, along with associated metadata, and will share it with the TVS. The TVS will create templates from the photos and use the templates to supplement a gallery of templates of known identities for the traveler. The TECS System primary arrival application may also rely on a TVS gallery. The list of sea ports of entry where TVS is deployed is available at https://www.cbp.gov/travel/biometrics (see "Experience it Here").

## 6. Seaport Exit

There are currently no biometric capabilities deployed for sea exit environments.

# Appendix B: Partner Owned and Operated Camera Collection Sites

*Last Updated: November 14, 2018*

In 2017, CBP announced new and expanded partnerships with commercial air carriers and airport authorities to capture facial images of travelers and send those photographs to CBP for matching against previously-captured photos, using the TVS. By using biometric technologies in voluntary partnerships with other federal agencies and commercial stakeholders, CBP is facilitating a large-scale transformation to make travel more secure and enhance the integrity of the immigration system. These partnerships enable CBP to more effectively verify the identities of individuals entering and exiting the United States, identify foreign nationals who are violating the terms of their admission, and expedite immediate action when such violations are identified.

In some arrangements, an airline or airport authority partner staffs the TVS biometric collection and boarding process, rather than CBPO. 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 identity verification. Based on pre-arranged agreements with CBP, these stakeholders deploy their own camera operators and camera technology meeting 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 via a secure, encrypted connection. While the photo capture process may vary slightly according to the unique requirements of each participating airline and airport authority, the IT infrastructure supporting the backend process is the same.

During boarding, each traveler stands for a photo in front of a partner-provided camera. Aided by the authorized airline or airport personnel, the partner-owned camera attempts to capture a usable image and submits the image, sometimes through an authorized integration platform or vendor, to CBP's cloud-based TVS facial matching service. TVS then generates a template from the departure photo and uses that template to search the assembly of historical photo templates in the cloud-based gallery. Some airlines continue to accept boarding passes at the gate, while other carriers accept CBP's biometric identity verification in lieu of boarding passes as part of a new paperless, self-boarding process. In the latter process, the carrier may employ technologies (such as automated gates) to further automate the process of directing the traveler, whose photo generated a positive match with a photo in the gallery, to board the plane.

**U.S. Air Exit Airports (includes month of initial deployment):**

- Orlando, FL (MCO), British Airways: January 2018
- Atlanta, GA (ATL), Delta Airlines: August 2017
- Detroit, MI (DET), Delta Airlines: July 201

- Washington, DC – Dulles (IAD), Metropolitan Washington Airports Authority: August 2018
- Los Angeles, CA (LAX), Los Angeles World Airports: January 2018

# Appendix C: Other Government Agency Owned and Operated Camera Collection Sites

*Last Updated: November 14, 2018*

## 1. Transportation Security Administration (TSA)

In addition to deploying TVS at the boarding gate, CBP has been working with the Transportation Security Administration (TSA) to test the TVS process for verifying traveler identities using the TVS camera technology and matching services at the TSA security screening checkpoint.[82] Standard TSA security screening procedures have required manual identity checks by the TSO. A recent technical demonstration, which served as a variation of the TVS exit process, leveraged the technologies to automate what has typically been a manual identity verification process for travelers. This demonstration used the APIS manifest data to create a gallery of travelers scheduled to board specified outbound international flights during a defined period. During 2017, CBP and TSA began this first phase, which evaluated the technology and matching process at the TSA checkpoint.

CBP and TSA are now testing a process in which the Transportation Security Officer (TSO), who serves as the TSA Travel Document Checker, directs the international outbound travelers to a CBP-owned camera, which is placed near the podium at the TSA checkpoint for a photo capture.[83] Once the photo is captured and transmitted to the TVS matching service, the TVS converts the photo into a template and matches it against the gallery of the predetermined set of templates of historical images that are already stored in the TVS cloud. The TSO will receive the result of this matching process via a mobile-friendly dashboard application developed by CBP for TSA, which is only accessible on the DHS network and only to authorized TSOs using TSA-issued devices. If the TVS confirms the traveler's identity, the CBP dashboard application will display the newly-captured image, along with biographic data (full name and date of birth) of that traveler, for review by the TSO, who will direct the traveler to the appropriate screening lane based on TSA's standard security screening procedures.

If the TVS cannot capture an acceptable image of the passenger, or there is no match for the traveler's photo, the TSA tablet will display only the captured photo but no biographic information, the TSO will follow TSA's standard procedures for verifying the traveler's identity, and the traveler will proceed to the appropriate screening lane. In addition, CBPOs receive an alert on the BE-Mobile device indicating that for a particular traveler, there was not a match. For in-scope travelers, the CBPO may use the BE-Mobile device to verify authenticity, identity, and citizenship via biographic data and an examination of travel documents. The CBPO can also use

[82] See DHS/CBP/PIA-030(d) Traveler Verification Service (TVS) (September 25, 2017), available at www.dhs.gov/privacy.
[83] TSOs will be trained to operate the cameras, which are owned by CBP.

the device to determine the appropriate course of action(s) for biometric capture or exemption, i.e., through new fingerprints, photo captures, and/or the collection of additional biometric information from the traveler. During this process, if the CBPO identifies actionable derogatory information on a particular traveler, (e.g., the individual is found on the IDENT biometric watch list), the CBPO may escort the traveler to the FIS area to conduct further questioning or appropriate actions under CBP's law enforcement authorities.

Several attempts may be made to capture a high quality photo of each traveler. Ultimately, if the TVS matching process is unable to verify the traveler's identity, that is, if TVS cannot capture an acceptable image of the traveler (i.e., the image quality is particularly low), or there is no match for the traveler's photo, the TSA mobile device will display only the captured photo but no biographic information, and the TSO will follow TSA's standard procedures for verifying the traveler's identity. In addition, the TSO may request that the traveler proceed to exception processing with one of the CBPOs, who are assigned to each TSA checkpoint, to adjudicate issues resulting from the TVS matching process. If the traveler approaches a CBPO, the CBPO may examine travel documents in order to verify authenticity, identity, and citizenship. CBPOs may also access referrals of foreign nationals in Biometric Exit Mobile Application (BE-Mobile) devices to adjudicate referred TVS "no matches" and determine the appropriate course of action(s) for biometric capture or exemption. This process requires additional information from the traveler, such as a passport, and new fingerprints or photo captures. CBP may use all biographic and biometric information provided by the traveler during the encounter to search law enforcement databases for relevant information about the traveler.

Each traveler's biographic and biometric data is purged from the TSA-issued device, either at the time of the next traveler's transaction or after two minutes, whichever occurs first. All PII collected for the TVS transaction is stored in a secure database within the CBP network. CBP does not retain the images of U.S. citizens once their identities are verified. Photos of non-U.S. citizens are retained for 14 days with ATS-UPAX and are shared with IDENT. In addition, within a short time, CBP purges all photos, regardless of immigration or citizenship status, from the TVS cloud matching service.[84] 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, alternative procedures, and Frequently Asked Questions. Individuals who wish not to participate may request alternative processing by a TSO.

[84] Photos of all travelers are retained in secure the TVS cloud for no more than 12 hours after identity verification, in case of an extended system outage.

# Appendix D: International Biometric Entry/Exit Partnerships

*Last Updated: November 14, 2018*

CBP is developing global biometric partnerships in order to share facial images, as appropriate, in order to enhance security and expedite international travel. CBP will leverage biometric data collected by a partnering country's arrival process and use the shared information to record a biometric exit from the U.S., thus facilitating the ability to confirm a biometric departure without major investments in infrastructure. Additionally, this initiative can be particularly useful for CBP in verifying the identity of first-time Visa Waiver Program travelers, for whom CBP has no photo available. By obtaining a photo in advance from the partner, CBP can close this gap and verify the identity of the traveler. CBP is developing programs with select international airlines and foreign countries, in which the international partner collects the photos of travelers to the United States at the airport of origin and securely transmits the facial images to CBP. CBP will update this appendix once sharing arrangements with partners are in place.