Privacy Impact Assessment Update
for the

Traveler Verification Service (TVS)

DHS/CBP/PIA-030(b)

May 15, 2017

Contact Point
Kim A. Mills
Planning, Program Analysis and Evaluation (PPAE)
Office of Field Operations
U.S. Customs & Border Protection
(202) 344-3007

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

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is implementing the Traveler Verification Service (TVS) to continue the development and expansion of a biometric entry-exit system for international flights at airports throughout the United States. Similar to the Departure Verification System (DVS),[1] the TVS uses facial matching to verify the identities of travelers on select flights, but uses a cloud environment for facial matching. CBP is publishing this updated Privacy Impact Assessment (PIA) to provide the public with notice of how the TVS collects, uses, and maintains personally identifiable information (PII).

Overview

The 1996 Illegal Immigration Reform and Immigrant Responsibility Act[2] called for the creation of an automated system to record arrivals and departures of non-U.S. citizens at all air, sea, and land ports of entry. The 2002 Enhanced Border Security and Visa Entry Reform Act,[3] the Intelligence Reform and Terrorism Prevention Act of 2004,[4] and the Implementing Recommendations of the 9/11 Commission Act of 2007[5] all called for the creation of a nationwide biometric entry-exit system. Although biometric screening on entry has been in place since 2004,[6] U.S. Customs and Border Protection (CBP) has continued to develop and test various systems and processes in order to identify a method for comprehensive biometric exit screening, including the creation of exit records for individuals departing the United States. Since being tasked with the biometric exit mission in 2013, CBP has been fully committed to developing and testing new processes and capabilities for biometrically recording persons leaving the United States through the use of facial recognition technology. The *Consolidated Appropriations Act of 2016*[7] 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 U.S. Department of Homeland Security (DHS) to "expedite the completion and implementation of a biometric entry-exit tracking system for in-scope travelers to the United States."[8]

---

[1] *See* DHS/CBP/PIA-030(a) Departure Verification System (December 16, 2016), *available at* https://www.dhs.gov/privacy.
[2] Pub. L. 104-208.
[3] Pub. L. 107-173.
[4] Pub. L. 108-458.
[5] Pub. L. 110-53.
[6] *See* DHS/NPPD/PIA-001 US-VISIT Program, Increment 1 (January 16, 2004), *available at* https://www.dhs.gov/privacy.
[7] Pub. L. 114-113.
[8] Executive Order 13780, *Protecting the Nation from Foreign Terrorist Entry into the United States*, 82 FR 13209

By partnering with stakeholders on a voluntary basis and using biometric technologies, CBP is facilitating a large-scale transformation of air travel that will make air travel more: (1) secure, by providing increased certainty as to the identity of airline travelers at multiple points in the travel process; (2) predictable, by establishing a clear, easily-understood process that will reduce the potential for major "bottlenecks" within the air travel process; and (3) able to build additional integrity to the immigration system, by better identifying which foreign nationals are violating the terms of their admission to the United States, and by providing capability for immediate action when that occurs.

Departure Information System Test

In June 2016, CBP began to pilot the Departure Information System Test (DIST)[9] to assess whether facial comparison technology could be used to 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. The test was scoped to include only one route and run until September 30, 2016; the pilot was later extended through November 2016. For flights operating on this route, a CBP-manned camera and tablet computer were placed between the boarding pass reader and the aircraft. As travelers checked in for their flight, CBP obtained passenger manifest data.[10] CBP generated biometric templates[11] from existing travelers' photographs and assembled the templates into a downloadable file, which was pushed to the tablet prior to boarding. As travelers passed through the boarding area, the camera took their photographs. The real-time photographs were then compared with the expected travelers' downloaded biometric (photo) templates to determine if CBP systems could accurately match live photographs with previously-acquired photos of the same traveler. CBP used the pilot to assess these matching capabilities; no exit records were created. Images were stored on the tablet for the duration of the flight, after which time the photos were purged.

Departure Verification System

The Departure Verification System (DVS), which operationalized the DIST pilot, follows

(March 9, 2017), *available at* https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states.

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

[10] *See* DHS/CBP/PIA-001 Advance Passenger Information System (June 5, 2013), *available at* https://www.dhs.gov/privacy.

[11] 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.

the same process as DIST. At selected departure gates at select airports, CBP deploys a facial recognition camera in close proximity to the airline boarding pass reader. This camera matches live images with existing photo templates from passenger travel documents. CBP assembles these photo templates based on Advance Passenger Information System (APIS)[12] flight manifest data for U.S. citizens and non-U.S. citizens who are scheduled to board the upcoming flight. Upon receipt of APIS manifest data and throughout the passenger check-in process, CBP compiles photos from various sources in the Automated Targeting System (ATS)[13] Unified Passenger Module (UPAX). The CBP Officer staffing the boarding gate uploads the group of templates onto a tablet computer prior to flight boarding. At the gate, an airline operator scans the traveler's boarding pass, and the camera takes a photo of the traveler. Signage posted in close proximity to the camera demonstrates how to interact with the device.

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 the passenger loading bridge. If the image created by the facial recognition camera system does not match the photograph template on file that is associated with the individual's travel document, the operator directs the traveler to a CBP Officer stationed at the passenger loading bridge. The CBP Officer uses a wireless handheld device[14] to verify the traveler's identity using either fingerprints for aliens, via a query in the Automated Biometric Identification System (IDENT),[15] or by conducting an inspection to ensure the traveler is holding valid travel documents. If the CBP Officer is unable to locate a record of the traveler's fingerprints in IDENT, the officer runs a separate criminal history check in the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS)[16] and enrolls the fingerprints in IDENT.

As CBP verifies the identity of the travelers, either through automated facial recognition or manual officer processing, the CBP Officer transmits information back to the respective CBP systems. CBP retains facial images of non-immigrant aliens, lawful permanent residents, and U.S. citizens for no more than two weeks for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. CBP retains biographic exit records from the boarding pass for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens. Retention policies follow the Border Crossing Information

---

[12] *See* DHS/CBP-005 Advance Passenger Information System, 80 FR 13407 (March 13, 2015).
[13] *See* DHS/CBP/PIA-006 Automated Targeting System (January 13, 2017), *available at* https://www.dhs.gov/privacy.
[14] *See* DHS/CBP/PIA-026 Biometric Exit Mobile Air Test (BE-Mobile) (June 18, 2015), *available at* https://www.dhs.gov/privacy.
[15] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.
[16] *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.

(BCI) System of Records Notice (SORN)[17] for U.S. citizens and lawful permanent residents and the Nonimmigrant Information System (NIIS) SORN[18] for non-immigrant aliens. However, records retained in association with a law enforcement action are retained for 75 years, consistent with the TECS SORN.[19]

Reason for the PIA Update

CBP is publishing this updated PIA to provide notice of the TVS, an enhancement to the DVS process that will reduce the need for CBP Officers to mitigate verification issues and will improve response times for matching photos. Overall, the TVS represents two significant changes from the process established under the DVS: (1) the temporary storage of traveler photos in a secure, approved public and commercial Virtual Private Cloud (VPC)[20] environment; and (2) the use of a cloud-based biometric matching service[21] to compare photos.

Traveler Verification Service

Similarly to operations of the DVS, the TVS will use CBP's biographic APIS manifest data and existing photographs of U.S. citizen and non-U.S. citizen travelers boarding international flights in order to confirm the identity of the traveler, create an exit record, and biometrically confirm the exit of in-scope[22] non-U.S. citizens. The APIS manifest, which contains information collected by airlines and transmitted to CBP prior to departure, consists of biographic information such as the name, date of birth, country of citizenship, passport information (number, country of issuance, and expiration date), and an airline-generated alphanumeric unique ID (UID).[23] The manifest also includes specific details of the traveler's itinerary, such as flight number, carrier, originating airport, and destination airport.

Under the TVS process, ATS-UPAX will generate biometric templates of the historical images of travelers for a given flight and will temporarily store those templates, but not the actual

[17] *See* DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[18] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015).
[19] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).
[20] CBP uses a commercial Virtual Private Cloud (VPC) that is a logically isolated (walled-off) virtual network over which CBP administers control.
[21] The biometric facial matching service uses a learning-based visual search and image classification software to search and compare facial images, and detect similar faces within a large gallery of templates.
[22] An "in-scope" traveler is any person who is required by law to provide biometrics upon entry to the United States, pursuant to 8 CFR 235.1(f)(ii).
[23] 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.

images, in the VPC prior to boarding. These images include photographs captured by CBP during the entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters.[24]

As boarding begins, each traveler approaches the departure gate to present a boarding pass and stand for a photo in front of a CBP-owned camera, each of which will be connected to the VPC via a secure, encrypted connection. Once the camera captures a usable image, it will submit the image to CBP's cloud-based backend facial matching service via an HTTPS/SSL-encrypted connection. The matching service will then generate a template from the departure image and use that template to search the assembly of historical photo templates. The matching service will return faces that best match the reference face, thus verifying the identities of individual travelers. If a match is found between the newly-captured image template and the pool of previously-captured image templates, a light will signal the match, and CBP (or in some cases, a trained representative from the airline or airport) will direct the traveler to proceed to the aircraft. If the camera is unable to capture a satisfactory image within a reasonable amount of time, the traveler will be required to stand for another photo. If, after repeated attempts, the identity of the traveler cannot be verified, a CBP Officer will escort the traveler from the immediate area and attempt to verify his or her identity using alternative methods.

As CBP verifies the identity of the travelers, either through automated facial recognition or manual officer exception processing, the backend matching service returns the "match/no-match" results, along with the respective associated UID, to ATS-UPAX. Similar to the DVS, CBP creates a record of the traveler's departure from the United States in APIS, which updates the traveler record from "reported" to "confirmed." CBP also retains entry and exit records in the Arrival and Departure Information System (ADIS) for lawful permanent residents and non-immigrant aliens, consistent with the ADIS SORN.[25] CBP will continue to retain biographic exit records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens, consistent with the BCI[26] and NIIS[27] SORNs, respectively. However, records associated with a law enforcement action are retained for 75 years, consistent with the TECS SORN.[28]

CBP will temporarily retain all photos within the isolated part of ATS-UPAX to support system audits, to evaluate the TVS facial recognition technology, and to ensure accuracy of the

---

[24] 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.
[25] See DHS/CBP-021 Arrival and Departure Information System, 80 FR 72081 (November 18, 2005).
[26] See DHS/CBP-007 Border Crossing Information, 81 FR 4040 (January 25, 2016).
[27] *See* DHS/CBP-016 Nonimmigrant Information System, 80 FR 13398 (March 13, 2015).
[28] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008).

facial recognition algorithms. CBP staff will manually review system-generated matches related to the identification of a U.S. citizen in order to confirm that the match was correctly made. All newly-captured photos and templates will be deleted from ATS-UPAX within 14 days but will be deleted from the VPC no later than after the conclusion of the flight. The VPC does not store either photos or templates permanently.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information, and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII).[29] The Homeland Security Act of 2002, Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[30] and the Homeland Security Act of 2002, Section 222.[31] This PIA Update examines the privacy impact of the TVS and collection of facial image and boarding pass biographic data as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

There has been no change to transparency since the original PIA. As CBP expands upon the DVS via the TVS, it will continue to provide notice through posted signs to individuals whose facial images are captured. International travelers are subject to the laws and regulations enforced

[29] 5 U.S.C. § 552a, *as amended.*
[30] 44 U.S.C. § 3501 note.
[31] 6 U.S.C. § 142.

or administered by CBP when they travel internationally and may be inspected. When CBP captures the departure photos, signs inform the public that CBP will be capturing the photos and refers travelers who have questions to the CBP Information Center. In addition, CBP posts signs in boarding areas informing individuals of possible searches, and the purpose for those searches, upon arrival or departure from the United States. Upon request, individuals will be provided a tear sheet with additional information on the project, including the legal authority and purpose for inspection, the routine uses, and the consequences for failing to provide information.

Information on this and other CBP biometric exit projects is available on the official CBP public website; CBP will issue press releases and update its website as it deploys new biometric exit processes at new airports.[32] CBP provides additional notice to the public through this PIA Update and will publish updates or additional PIAs for future changes.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

The TVS relies upon information collected directly from the individual (the photograph captured during the boarding process) as well as information collected from the airline (via the APIS manifest) and photographs collected previously by CBP, DHS, or the Department of State. Because CBP is charged with collecting biometric information from in-scope travelers and because CBP has an enforcement interest in ensuring all travelers are in possession of valid travel documents, travelers are not allowed to opt-out of the TVS process. However, if a U.S. citizen requests not to participate in the TVS, his or her identity may be verified by an available CBP Officer via manual processing.

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

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20002

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

Fax Number: (202) 325-1476

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

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

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

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

Privacy Risk: There is a risk to individual participation because individuals may be denied boarding if they refuse to submit to biometric identity verification under the TVS.

Mitigation: This privacy risk cannot be fully mitigated. Although the redress and access procedures above provide for an individual's ability to correct his or her information, the only way for an individual to ensure he or she is not subject to collection of biometric information when traveling internationally is to refrain from traveling. Individuals seeking to travel internationally are subject to the laws and regulations enforced by CBP and are subject to inspection. If a U.S. citizen, however, requests not to participate in the TVS, an available CBP Officer may use manual processing to verify the individual's identity. Upon request, individuals will be provided a tear sheet to provide more information on the project. In addition, individuals may file an inquiry to seek redress through DHS TRIP.

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for records collected pursuant to the TVS 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.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The purpose of the TVS has not changed since the publication of the DVS PIA Update. The information collected under the TVS will be used to verify travelers' identities and create exit records, as described in the overview section of this document. Although CBP has previously collected biographical PII from the airlines through the APIS manifest and collected biometric information from certain travelers on arrival to the United States, collecting images of travelers via the TVS will expedite identity verification and enhance security. In addition to issuing this PIA, CBP is updating its regulation to address the systematic collection of biometrics from all travelers, U.S. citizens and lawful permanent residents, at ports of entry throughout the country under the TVS.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The TVS collects facial images and biographic data from departing air travelers on select flights. CBP retains both U.S. citizen and non-U.S. citizen photos, linked with their respective

UIDs, for up to two weeks in order to review and confirm the match, evaluate the facial recognition technology, ensure accuracy of the algorithms, and support system audits. After each flight, the VPC will delete all facial images. CBP will continue to retain biographic exit records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-immigrant aliens, consistent with the BCI[33] and NIIS[34] SORNs. However, records retained in association with a law enforcement action are retained for 75 years, consistent with the TECS SORN.[35]

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

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

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

CBP will use the information it collects under the TVS to create exit records, as described in the overview section of this document. CBP will share entry and exit data consistent with the terms described in the relevant SORNs listed above. Only CBP Officers and other personnel with a need to know may view the photos when the situation warrants a review. No airline personnel are given the opportunity to view the photos.

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

Mitigation: This risk is partially mitigated. CBP 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. However, although CBP does not share the facial images with the airlines, it does share the images, in the form of irreversible photo templates, with the VPC for the purpose of matching travelers with previous photos and thus

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

verifying their identities. CBP requires that the VPC delete all photos after the flight has departed, and no later than when the flight has concluded. CBP may also share information with federal, state, and local authorities, which may be authorized to use the information for purposes beyond the scope of CBP's mission. CBP provides notice of this sharing in its various SORNs, which are detailed in the original DIST PIA. CBP uses and shares information consistent with these SORNs and updates these notices for any new uses.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

CBP uses biometric technologies to meet the need for ensuring accurate, relevant, timely, and complete identity verification for travelers. To enhance the accuracy of matching, CBP has developed technical specification requirements for camera vendors because the quality of facial images dramatically impacts the performance of all facial recognition algorithms. The National Institute of Standards and Technology (NIST) has shown that the accuracy (true acceptance rate, or TAR) of a picture captured in a well-controlled environment, such as a passport photo, is of significantly higher quality than for a picture taken in an unstructured environment (for example, with a poor quality web cam). CBP requires facial images captured at the departure gate to conform closely to the International Civil Aviation Organization (ICAO) standards (ISO 19794-5)[36] 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.[37]

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

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,

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

academic, and government algorithms in matching facial photographs. S&T is generating a report identifying how each algorithm performed as a true positive rate, false positive rate, false match rate, and false non-match rate.

Privacy Risk: There is a risk that CBP's cameras will be unable to capture images of high enough quality to produce accurate matches, resulting in CBP's inability to confirm traveler identities.

Mitigation: This risk is mitigated. CBP requires its cameras to meet ANSI/NIST and international standards as well as an accuracy goal of 96% TAR. In addition, TVS cameras are required to (1) capture multiple images; (2) draw the traveler's attention to the camera and hold the traveler's attention throughout the capture process, and alter the traveler's position when the process is complete; (3) include a "time-out" function in order to send the best-captured image of the traveler if no image was able to meet the desired quality threshold; and (4) provide proper lighting. If, for any reason, the identity of the traveler cannot be verified after repeated attempts, a CBP Officer may be contacted in order to verify identity using alternative methods. During manual processing, an officer manually verifies the authenticity of the documentation, such as the passport, and manually verifies that the traveler matches the passport. If the officer is concerned about the authenticity of the documents or the identity of the individual, he or she may swipe the passport through a Biometric Exit (BE) Mobile[38] device.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

CBP will store TVS information in secure CBP systems and temporarily in a secure VPC environment. 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 uses a virtual private network (VPN) with two-factor authentication and strong HTTPS/SSL encryption to transfer the data between the camera, the VPC, and CBP systems as well as for PII at rest.

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

The cloud service provider (CSP) selected for this initiative will adhere to the security and privacy controls required by NIST Special Publication 800-144, "Guidelines on Security and Privacy in Public Cloud Computing,"[39] and the DHS Chief Information Officer.

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

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

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

Mitigation: This risk partially mitigated. CBP will secure the TVS cloud environment according to NIST and DHS security controls. Additionally, CBP utilizes strong HTTPS/SSL encryption in order to secure the data both at rest and in transit, such as during the data transfers between the cameras, the cloud, and CBP systems. Despite these precautions, there remains some risk of an unauthorized user gaining access to the data in the VPC. However, additional controls mitigate the potential for harm. The VPC houses only a biometric template, which cannot be reverse engineered for viewing by unauthorized users; accordingly, any data accessed in an unauthorized fashion would be unrecognizable and virtually unusable.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All CBP personnel with access to the data are required to complete annual cyber security and privacy awareness training in addition to training on ethics and the CBP Code of Conduct. CBP employees and contractors must pass a full background investigation and must also be trained regarding the access, use, maintenance, and dissemination of PII before being given access to the

[39] For more information, please *see* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

system(s) maintaining the facial image data. Access controls, including technologic controls, will ensure only authorized access to the facial image data, which will not be accessed or released for any unauthorized use. Additionally, CBP will document the deletion of data from ATS-UPAX and the CSP. Finally, the CBP Privacy Office, in collaboration with the CBP Office of Field Operations, will monitor the implementation of the TVS process in collaboration with airline and airport partners to ensure that all parties are complying with the privacy protections documented in this PIA.

Responsible Officials

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

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

Approval Signature Page

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

_____

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