Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form will be used to determine whether a Privacy Impact Assessment (PIA), System of Records Notice (SORN), or other privacy compliance documentation is required under the E-Government Act of 2002, the Homeland Security Act of 2002, the Privacy Act of 1974, or DHS policy.

Please complete this form and send it to your Component Privacy Office. If you are unsure of your Component Privacy Office contact information, please visit https://www.dhs.gov/privacy-office-contacts. If you do not have a Component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
DHS Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717

PIA@hq.dhs.gov

Your Component Privacy Office will submit the PTA on behalf of your office. Upon receipt from your Component Privacy Office, the DHS Privacy Office will review this form. If a PIA, SORN, or other privacy compliance documentation is required, your Component Privacy Office, in consultation with the DHS Privacy Office, will send you a copy of the template to complete and return.

For more information about the DHS Privacy compliance process, please see https://www.dhs.gov/compliance. A copy of the template is available on DHS Connect at (b)(7)(E) or directly from the DHS Privacy Office via email: PIA@hq.dhs.gov or phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project, Program, or System Name:	**TVS Identity Verification for Select International Flights En-route to the U.S. and Facial Comparison for APIS Compliance Test**		
Component or Office:	**Customs and Border Protection (CBP)**	**Office or Program:**	**Office of Field Operations (OFO), Admissibility and Passenger Programs (APP)**
FISMA Name (if applicable):	**Traveler Verification Service**	**FISMA Number (if applicable):**	**CBP-07658-MAJ-07658**
Type of Project or Program:	**Program**	**Project or program status:**	**Update**
Date first developed:	**April 1, 2016**	**Pilot launch date:**	**January 2, 2019**
Date of last PTA update	**N/A**	**Pilot end date:**	**N/A**
ATO Status (if applicable):[1]	**Complete**	**Expected ATO/ATP/OA date (if applicable):**	Click here to enter a date.

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b) (6) (b) (7) (c) [redacted]		
Office:	OFO/APP	**Title:**	Director
Phone:	(b) (6) (b) (7) (c) [redacted]	**Email:**	(b) (6) (b) (7) (c) [redacted]@cbp.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b) (6) (b) (7) (c) [redacted]		
Phone:	(b) (6) (b) (7) (c) [redacted]	**Email:**	(b) (6) (b) (7) (c) [redacted]@associates.cbp.dhs.gov

[1] The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see

(b)(7)(E) [redacted]

1. Reason for submitting the PTA: Updated PTA

U.S. Customs and Border Protection (CBP), Office of Field Operations (OFO), Admissibility and Passenger Programs (APP), is submitting this updated Foreign Boarding PTA. CBP is expanding on existing biometric capabilities available with CBP's Traveler Verification System (TVS) to include utilizing TVS during the boarding process on an incoming international flight at foreign airports. This allows CBP to biometrically confirm a traveler's identity during his/her journey to the U.S. The process may be utilized during the airline identity verification process, at the departure gate for flights destined to the United States from foreign.

This PTA consolidates two previously adjudicated PTAs: (1) TVS Identity Verification at Foreign Airports (adjudicated on 8/6/2019), (2) APIS-TVS Facial Comparison Test (adjudicated on 11/12/2021).

Foreign Boarding (APIS Compliance Test)

Under this test, participating carriers utilize the TVS facial comparison service to ensure the manifest information transmitted to CBP is correct and to perform the required identity verification. Carriers enroute to the United States who voluntarily participate in this test must collect and submit photos via TVS at the time of boarding but may also collect and submit photos at passenger check-in for flights directly to or from the United States. The purpose of the APIS test is to determine the feasibility of allowing carriers to use CBP's TVS facial comparison service to comply with the carrier's APIS verification requirements. Facial Comparison for APIS Compliance Test was published in the Federal Register on 02/16/2023 under 88 FR10137. The test is expected to run for approximately two years. CBP is accepting applications to participate in the test on a rolling basis throughout the two-year testing period.

Test Process

The Facial Comparison for APIS Compliance test is voluntary. Eligible carriers who voluntarily participate in this test collect facial images (photographs) of certain travelers at the gate when boarding or at other identity check points. The carriers will then submit those facial images to CBP's TVS facial comparison service. The submitted photographs are compared to biometric templates generated from pre-existing photographs that CBP already maintains, known as a "gallery," as described below.[2]

When CBP receives a passenger manifest, CBP will build a gallery of photographs for the individuals identified on the manifest. These images may include photographs captured by CBP during previous entry inspections, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters. If TVS matches the traveler's facial image to a photograph in the gallery and the manifest information transmitted to CBP is correct, the carrier's APIS verification requirements will be considered fulfilled and the carrier will not need to perform any additional identity or passenger manifest verification.[3] If the traveler's facial image does not result in a match from TVS for any reason, the carrier will be required to verify the traveler's identity through a manual review of the traveler's travel documents pursuant to the existing APIS regulatory requirements. If a carrier identifies a traveler who has been incorrectly matched

[2] 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. CBP builds "galleries" of photographs based on where and when a traveler will enter, exit, or check-in. If CBP has access to advance passenger manifest information, CBP will build galleries of photographs based on upcoming flight or vessel arrivals or departures. CBP creates localized photographic galleries using APIS data. To populate the localized galleries with photographs, CBP compiles photographs from existing CBP sources. TVS will then generate biometric templates for each gallery photograph and store the template, but not the actual photograph, in the TVS virtual private cloud (VPC) for matching when the traveler arrives or departs.

[3] Carriers still need to ensure that each traveler has a valid passport or authorized travel document in his or her possession. This fulfills the passenger manifest requirements for the United States, but there may be additional requirements from destination or transit countries.

by the TVS to another passenger (referred to as a "false positive"), the carrier will manually review the travel documents of any such false positives pursuant to current APIS requirements.[4]

Foreign Boarding for flights Enroute to the U.S. and Other TVS Identity Verification at Foreign Airports

At select foreign airports, to confirm the identity of the traveler, CBP will assemble a gallery of photographs using TVS to create biometric templates from those photos, and stages them, along with a unique identifier (UID)—generated by the Advance Passenger Information System (APIS)—to the TVS. TVS assembles this gallery of photos from travelers' historical documents, based upon the APIS manifest of travelers departing on pre-selected flight(s) enroute to the U.S. The airline will take a photo of the traveler's face and transmit the image to TVS, which will create a template of that image and match it against templates of previous photos assembled from previous DHS holdings. If the traveler is positively matched, the result will be shared with the airline partner, along with the UID, and the traveler may be permitted to continue with either the Preclearance process or boarding the flight, depending on the environment. If the traveler is not matched, he or she will be processed manually by an airline agent and will be allowed to board the flight if the traveler matches his or her identity document. If the traveler does not match his or her identity document, the carrier would deny boarding on the flight to that individual.

As per the current Preclearance process, to account for travelers who do not board flights enroute to the U.S. from Preclearance locations, a CBP Officer will amend the crossing record in TECS for those who do not board the flight. For non-Preclearance locations that use the TVS for identity verification of travelers enroute to the U.S., no encounter crossing record is created within TECS unless and until the traveler arrives at the U.S. Port of Entry and is processed by CBP; however, a record of all transactions is stored in a boarding event table within the ATS database. This table is a backend table and is not accessible to general users. The only way to search this table is by date; information from the table cannot be retrieved by a personal identifier.

Notice

For Foreign Boarding, Uses of TVS at Foreign Airports and the Facial Comparison for APIS Compliance Test, if an individual traveler, regardless of citizenship, does not want to be photographed, the traveler can opt out of this procedure by notifying the carrier. CBP requires carriers to post signs notifying travelers of their ability to opt out. Additionally, carriers may choose to give a verbal announcement during the boarding process and/or pass out tear sheets with additional information about CBP's use of facial comparison technology. If a traveler opts out, the carrier must perform a manual review of the travel documents to ensure the manifest information sent to CBP is correct and verify the traveler's identity.

Retention

For Foreign Boarding as well as APIS Compliance Test, photos of U.S. citizens are deleted immediately upon confirmation of U.S. citizenship, but no later than 12 hours only under specific circumstances. If there is a system or network issue, photos will reside in an inaccessible queue for up to 12 hours and will be processed once the system and/or network connectivity is re-established, and proper dispositioning

[4] In the unlikely event that a false positive results in the creation of an incorrect travel record, the traveler affected by the incorrect travel record can seek redress through the DHS Traveler Redress Inquiry Program (DHS TRIP) at https://www.dhs.gov/dhs-trip or the CBP redress process, which can be found at https://www.cbp.gov/travel/international-visitors/i-94/traveler-compliance.

(confirmation of U.S. citizenship) can occur. CBP will retain photos of all noncitizens[5] and no matches for up to 14 days. Foreign Boarding Encounters are never sent or stored in IDENT.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information[6] ☒ Members of the public ☒ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons ☐ DHS Employees/Contractors (list Components): *Click here to enter text.* ☐ Other federal employees or contractors (list agencies): *Click here to enter text.*
2(a) Is information meant to be collected from or about sensitive/protected populations?	☒ No ☐ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[7] ☐ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

3. What specific information about individuals is collected, maintained, used, or disseminated?

CBP collects facial images as well as personal information from the APIS manifest, which is already being collected by the carriers. The following data elements are included in the manifest: name; date of birth; country of citizenship; and passport information (number, country of issuance and expiration date). In

[5] For purposes of this document, CBP uses the term "noncitizen" in place of the term "alien." However, CBP regulations use the term "alien."

[6] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

[7] This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at*

[redacted] (b)(7)(E)

addition, certain pieces of the traveler's itinerary will be collected, such as: flight number, carrier, originating port, and destination port.

For matching purposes, CBP will use templates of facial images from previous encounters with DHS or the Department of State, already available through TVS.

Specified partners, such as commercial air carriers, airport authorities, and cruise lines, collect the images of travelers and share the images with TVS, often through an integration platform or other vendor. These partners do not retain any photos. The TVS matching service converts the photos into secure templates and matches them against templates of previously captured images for identity verification.

CBP will capture images of travelers who do not opt-out; however, those images will not be stored and will be deleted once a match determination is made.

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?[8] If applicable, check all that apply.

☐ Social Security number ☐ Alien Number (A-Number) ☐ Tax Identification Number ☐ Visa Number ☒ Passport Number ☐ Bank Account, Credit Card, or other financial account number ☐ Driver's License/State ID Number	☐ Social Media Handle/ID ☐ Driver's License/State ID Number ☐ Biometric identifiers *(e.g., FIN, EID)* ☒ Biometrics.[9] *Please list modalities (e.g., fingerprints, DNA, iris scans):* **Facial Image Photograph** ☐ Other. *Please list: Click here to enter text.*
3(b) Please provide the specific legal basis for the collection of SSN:	N/A

3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.

N/A

3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[10] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or

[8] Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[9] If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS' IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

[10] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.

regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.*
N/A

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.[11] Please list all unique identifiers used: Facial Image template, APIS-generated Unique ID, APIS Manifest information (name, date of birth, travel document information) No border crossing records are created as part of this collection and all photos are destroyed. However, a transaction record is created which records some biographic information but it is not searchable by a unique identifier. ☐ By a non-unique identifier or other means. Please describe: *Click here to enter text.*

5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? *If no schedule has been approved, please provide proposed schedule or plans to determine it.* *Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.*[12]	CBP temporarily retains facial images of non-US citizens for no more than 14 days within TVS 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. 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. Photos of all travelers are purged from the TVS cloud matching service within 12 hours.. Foreign Boarding Encounters are never sent or stored in IDENT. CBP is currently updating the NARA retention schedule to include non-U.S. citizens and nonmatches. The approved NARA records schedule

[11] Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

[12] *See* (b)(7)(E)

	number for U.S. citizen encounter photos is DAA-0568-2019-0002.
5(a) How does the Project, Program, or System ensure that records are disposed of or deleted in accordance with the retention schedule (e.g., technical/automatic purge, manual audit)?	Deletion of traveler photographs/templates is verified during routine data analysis. CBP audits stakeholders periodically to ensure adherence to the retention policy. Furthermore, CBP's cloud service caches the data. The cache time is set via configuration within the cloud service provider's managed service. Additionally, the data cache is in an encrypted form and the cloud service provider does not have the encryption keys.

6. Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?[13]	☐ No. ☒ Yes. If yes, please list: CBP shares the facial images of in-scope travelers within DHS, with IDENT, and on occasion with S&T for testing purposes. CBP's ATS/UPAX, TECS System, ADIS, and APIS, DHS IDENT (only entry and exit encounters).
7. Does this Project, Program, or System connect, receive, or share PII with any external (non-DHS) government or non-government partners or systems?	☒ No. ☐ Yes. If yes, please list: *Click here to enter text.*
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? *If applicable, please provide agreement as an attachment.*	Existing Please describe applicable information sharing governance in place: *Click here to enter text.*
9. Does the Project, Program, or System or have a mechanism to track external disclosures of an individual's PII?	☐ No. What steps will be taken to develop and maintain the accounting: *Click here to enter text.* ☒ Yes. In what format is the accounting maintained: CBP has implemented Audit and monitoring tools like SIEM tool—Splunk, to ensure Auditing controls are met.

[13] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	□ Social Media □ Advanced analytics[14] □ Live PII data for testing ☒ No

[14] The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.

11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?[15] This does not include subject-based searches.	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

12. Does the planned effort include any interaction or intervention with human subjects[16] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for independent review and approval of this effort.[17]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:

[15] Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

(ii) the security of a Government computer system.

[16] Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

[17] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/compliance-assurance-program-office or https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.

14. Is there a FIPS 199 determination?[18]	☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☒ Moderate ☐ High ☐ Undefined

[18] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b) (6) (b) (7) (c)
Date submitted to Component Privacy Office:	**June 16, 2023**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	July 27, 2023

Component Privacy Office Recommendation:
Please include recommendation below, including what new privacy compliance documentation is needed, as well as any specific privacy risks/mitigations, as necessary.

(b) (5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6)
DHS Privacy Office Approver (if applicable):	Click here to enter text.
Workflow Number:	**0015052**
Date approved by DHS Privacy Office:	July 31, 2023
PTA Expiration Date	July 31, 2024

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	Program If "other" is selected, please describe: *Click here to enter text.*

Determination:	☐ Project, Program, System in compliance with full coverage ☒ Project, Program, System in compliance with interim coverage ☐ Project, Program, System in compliance until changes implemented ☐ Project, Program, System not in compliance
PIA:	**PIA update is required.** CBP/PIA-056 Traveler Verification System **[update required]**
SORN:	**System covered by existing SORN** DHS/CBP-007 Border Crossing Information (BCI), December 13, 2016, 81 FR 89957

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

(b) (5)