Homeland Security

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:	**Traveler Verification Service**		
Component or Office:	**Customs and Border Protection (CBP)**	**Office or Program:**	**Office of Field Operations**
FISMA Name (if applicable):	**Traveler Verification Service**	**FISMA Number (if applicable):**	**CBP-07658-MAJ-07658**
Type of Project or Program:	**System**	**Project or program status:**	**Existing**
Date first developed:	**April 1, 2016**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	**June 15, 2023**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable):[1]	**Complete**	**Expected ATO/ATP/OA date (if applicable):**	**December 5, 2023**

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b)(6) (b)(7)(C)		
Office:	**CBP/OFO/ISD/Biometrics Program Office**	**Title:**	**Director**
Phone:	(b)(6) (b)(7)(C)	**Email:**	(b)(6) (b)(7)(C) **@cbp.dhs.gov**

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6) (b)(7)(C)		
Phone:	(b)(6) (b)(7)(C)	**Email:**	(b)(6) (b)(7)(C) (b)(6) (b)(7)(C) **@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)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Renewal PTA

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, known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. Since the initial deployment of TVS, CBP has expanded TVS' uses of beyond the entry-exit process. In November 2018, CBP issued a comprehensive PIA, DHS/CBP/PIA-056, to comprehensively discuss TVS's use in the biometric entry-exit environment. In 2024, CBP plans to, update and rename the previously published DHS/CBP/PIA-056 TVS PIA to DHS/CBP/PIA-056 *Traveler Verification Service: Biometric Entry-Exit*. The renaming of the PIA will provide clarity on the scope of the PIA and also discuss the expanded capabilities and use cases in the biometric entry-exit environment. Separately, CBP plans to publish an additional PIA*:* DHS/CBP/PIA-08X *Traveler Verification Service* to discuss TVS as a service technology and the services TVS provides to CBP beyond the entry-exit environment and to partner agencies.

The last PTA was adjudicated on June 15, 2023, and expires on June 15, 2024. Although this PTA clarifies the scope of this PTA (in comparison to the TVS-I PTA), there are no major updates since the last adjudication.

<u>Background</u>

TVS is an accredited CBP information technology service 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.

TVS

TVS is the matching services in the external environment. The TVS external environment allows CBP's commercial clients (i.e., airlines, cruise lines) to call TVS matching services via a public ".com" endpoint.[2] TVS's technical stack is built using (b)(7)(E) s[3]. TVS makes use of services from TVS-I[4], particularly the Album Construction services which orchestrates the creating and maintaining of galleries. For example, an Air Exit gallery is built based on an APIS manifest which TVS Album Construction uses to generate a list of incoming travelers to a POE, TVS builds a gallery using photographs of past encounters or from other CBP holdings prior to inbound travelers arriving in the U.S.)[5]

Under the Federal Information Systems Management Act (FISMA), TVS has a system security plan that has been approved as part of the Certification and Accreditation (C&A) process. The most recent Authority to Operate (ATO) for TVS was completed in December 2023.

[2] This is projected to be migrated to a .gov by the end of CY 2024.

Biometric Galleries and Matching Process in the BEE environment

TVS stores biometric templates in a central repository called a *gallery*. The gallery is populated from existing CBP sources and system interfaces. These types of photographs include those captured by CBP during previous entry inspections, U.S. passports and U.S. visas, immigration records, and prior DHS apprehensions and encounters. The TVS then generates biometric templates for each gallery photograph and stores the template, but not the actual photograph, in the TVS virtual private cloud (VPC) for matching when the specific matching service is requested.

The content of the created gallery depends on the travel context (i.e., air and sea entry, air exit, the Transportation Security Administration (TS)] bag drop and security checkpoint locations) or the TVS matching service requested. TVS conducts the backend biometric matching and provides a result to the appropriate CBP interface depending on the environment.

As CBP's TVS receives the information with photographs to create a gallery, as referenced above, the photographs, are digitally templatized and added to the appropriate gallery for the life of the gallery until a call is made to TVS to initiate the facial matching.

The camera matches templates of the live images with existing photo templates from passenger travel documents. 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 a particular manifest, the traveler proceeds exits the United States. If the camera is unable to capture a satisfactory image within a reasonable amount of time, the traveler may be required to stand for another photo. If the identity of the traveler cannot be verified, whether after one photo capture attempt or multiple attempts, the traveler's identity will be verified using regular manual processing (i.e., comparing the traveler to their travel document photo) by either CBP or the gate agent, depending on the environment.

TVS Use Cases

The TVS external environment allows CBP's commercial clients (i.e., airlines, cruise lines) to call TVS matching services, rather than internal DHS users (e.g., CBP, ICE, TSA).

In 2017, CBP announced new and expanded partnerships with entities such as airport authorities, maritime port authorities, commercial air carriers, and maritime operators (e.g., cruise lines and cargo vessel operators) to take photos of travelers and submit them to CBP's TVS for matching against previously captured photos. 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 U.S. identify foreign nationals who are violating the terms of their admission and expedite immediate action when such violations are identified.

In some arrangements, a commercial carrier, vessel operator, or port authority partner operates the TVS biometric collection and boarding process, rather than a CBP officer. A number of authorized CBP partners, 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 connects to TVS via a secure, encrypted connection. While the photo capture process may vary slightly according to the unique requirements of each participating commercial carrier, operator, or port authority, the Information Technology (IT) infrastructure supporting the backend process remains the same.

TVS is used externally by commercial clients for the below use cases. Each of these uses cases are comprehensively covered in separate PTAs.

- **Air Exit:** On select flights, when boarding begins, each traveler approaches the departure gate to present a boarding pass and stands for a photo in front of an airline- or airport-owned camera, which connects 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.
- **Sea Entry:** Facial Biometric Debarkation is a public-private partnership that expands the use of facial biometrics into the debarkation process. Facial Biometric Debarkation is used to process arriving passengers on closed loop cruises. The Facial Biometric Debarkation process begins when cruise line passengers debark the cruise vessel at a U.S. seaport of entry. Cruise line passengers will pause for a photo that will be compared to images contained in CBP/DHS holdings to biometrically verify their identity. After a match response from the TVS, passengers are allowed to proceed through inspections and exit the terminal.
- **Sea Exit:** As passengers and crewmembers report at the vessel during embarkation, the cruise line will use their TVS-enabled cameras to capture a photo of the passenger or crewmember and send the photograph to the TVS for matching. If the match is successful, CBP creates a departure crossing record in CBP systems. This helps CBP to verify that vessel operators are accounting for their passengers and crewmembers.
- **Enhanced Passenger Processing/ Facial Biometric Embarkation:** When a traveler arrives at a U.S. port of entry that has an Enhanced Passenger Processing process available, eligible travelers proceed to the Enhanced Passenger Processing queue. Similar to Simplified Arrival, as part of the primary inspection, the traveler pauses for a photo at a partner owned camera. Enhanced Passenger Processing then biometrically confirms identity from pre-staged galleries based on the manifest in TVS. In addition to the biometric identity confirmation, Enhanced Passenger Processing validates that the traveler falls within a qualifying population by verifying citizenship, class of admission, and documents in the Department of State's Travel Document and Encounter Database. Enhanced Passenger Processing calls TECS to vet the traveler using their biographic information. Enhanced Passenger Processing displays a 'green' light to indicate to the CBP officer that the traveler is eligible and does not have any derogatory information in CBP holdings. A 'proceed' message is

displayed and the traveler continues. If the traveler is not eligible, does not match through TVS, officer discretion, and/or has derogatory information, a 'blue' light occurs, and the traveler receives a message stating "See Officer" for Simplified Arrival processing.

CBP uses TVS to verify the identity of international travelers exiting the U.S. TVS supports the air, sea, and land travel environments at ports of entry. The real-time capability to compare a traveler's live photograph to photographs stored in the document gallery. CBP assembles a localized pre-staged "gallery" of templates based on a travel manifest. CBP uses these "galleries" for matching purposes only. No live photographs of travelers are retained in CBP systems for more than 14 days. CBP collects these photographs to verify that the individual presenting themselves to confirm their departure from the U.S. is who they say they are. Additional information about CBP's use of TVS for identity verification in support of the biometric entry-exit process, is available in the forthcoming DHS/CBP/PIA-056 Traveler Verification Service Biometric Entry-Exit PIA series and appendices, and in the forthcoming DHS/CBP/PIA-0XX Simplified Arrival PIA.

Retention and Storage

With the operational deployment of TVS, CBP transmits facial images for in-scope travelers[3] to IDENT for retention as the traveler's biometric encounter with CBP. DHS already retains all entry photos of in-scope travelers in IDENT to create biometric records of entry for those travelers. 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 and can opt-out of the photo capture/facial recognition process. For U.S. citizens who do not opt out, CBP retains the image for no longer than 12 hours together with the confirmation of the crossing and the associated biographic information. U.S. citizens who do not wish to submit to facial photo capture pursuant to these processes may request alternative processing. Only photos of non-U.S. citizens are retained for the full 14 days in TVS and for the full retention period in IDENT.

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

[3] 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 nonimmigrant other than those specifically exempt as outlined in the CFR. Exempt nonimmigrants 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; nonimmigrants younger than 14 or older than 79 on the data of admission; nonimmigrants 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 nonimmigrants to whom the Secretary of Homeland Security and the Secretary of State jointly determine it shall not apply; or nonimmigrant to whom the Secretary of Homeland Security, the Secretary of State, or the Director of Central Intelligence determines it shall not apply.

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.

SORN Coverage

CBP maintains entry and exit records in accordance with the Border Crossing Information (BCI) SORN. CBP also retains entry and exit records in support of its immigration enforcement mission consistent with the Arrival and Departure Information System (ADIS) SORN. Biometric data stored in the Automated Targeting System (ATS) is covered by their source system SORNs (if applicable) or the ATS SORN, and records associated with a law enforcement action are stored in accordance with the TECS SORN. Additionally, additional uses cases that use TVS beyond biometric entry and exit operations may receive additional SORN coverage from the programmatic SORN that enables CBP to collect the photograph (e.g., ESTA SORN).

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[4] ☒ 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)[5]

[4] 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.

[5] 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

	☐ 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 collected by airlines, airport authorities, and cruise line operators. 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 addition, certain pieces of the traveler's itinerary will be collected, such as: flight number; carrier; originating airport (seaport); and destination airport (seaport).

In other air exit and seaport operations, CBP works with specified partners, such as commercial air carriers, 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. 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.

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?[6] 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	☐ Social Media Handle/ID ☐ Driver's License/State ID Number ☐ Biometric identifiers *(e.g., FIN, EID)* ☒ Biometrics.[7] *Please list modalities (e.g., fingerprints, DNA, iris scans):* **Facial Images** ☐ Other. *Please list: Click here to enter text.*
3(b) Please provide the specific legal basis for the collection of SSN:	N/A

Directive 002-02, Implementation of Section 1367 Information Provisions, *available at* (b)(7)(E)

[6] 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.

[7] 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.

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*,[8] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or 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.[9] Please list all unique identifiers used: Facial image template, APIS-generated Unique ID, APIS manifest information (name, date of birth, travel document information) ☐ 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.*[10]	TVS temporarily stores the photo template with the photo ID/traveler ID for the life of the gallery. The retention for this varies but, as an example use case for an air exit gallery, TVS typically stores the photo template/ID for 12 hours. However, TVS may need to retain the gallery for longer (e.g., due to flight delays). CBP is in the process of working with NARA to formalize a retention schedule for TVS. Under retention schedule DAA-0568-2022-0001, photographs of U.S. citizens captured by TVS that match a photograph in DHS holdings, are immediately deleted and no captured photographs are retained for no longer than 12 hours. Photographs

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

[9] 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.

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

	that are not matched, and are confirmed to be non-citizens, are retained for no longer than 14 days after match/no-match.
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?[11]	☐ No. ☒ Yes. If yes, please list: Under the TSA exit operations 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 to allow the traveler to proceed. CBP shares the facial images of in-scope travelers within DHS, with IDENT, and on occasion with S&T for testing purposes.
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: Although no PII is shared, CBP has partnered with NIST to test technologies developed by specified vendors and to evaluate algorithms on biometric projects. Under this partnership, NIST provided a positive/negative result after the matching analysis.
8. Is this sharing pursuant to new or existing information sharing agreement (MOU, MOA, LOI, RTA, etc.)? ***If***	Existing Please describe applicable information sharing governance in place: Each external partners is

[11] 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.

applicable, please provide agreement as an attachment.	required to review and sign a Business Requirements Document with CBP prior to the use of TVS.
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 implemented Audit and monitoring tools like SIEM tool – Splunk, to ensure Auditing controls are met.

10. Does this Project, Program, or System use or collect data involving or from any of the following technologies:	☐ Social Media ☐ Advanced analytics[12] ☐ Live PII data for testing ☒ No

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)?[13] 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,	☒ No.

[12] 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.

[13] 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.

how will the information be de-identified, aggregated, or otherwise privacy-protected?	☐ Yes. If yes, please elaborate

12. Does the planned effort include any interaction or intervention with human subjects[14] 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.[15]

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: *Click here to enter text.*

14. Is there a FIPS 199 determination?[16]	☐ 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

[14] 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.

[15] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/capo 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.

[16] 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. For more information, see https://www.nist.gov/itl/fips-general-information.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6) (b)(7)(C)
PRIVCATS ID Number:	**0017387**
Date submitted to Component Privacy Office:	**June 5, 2024**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	June 14, 2024
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.
PRIVCATS ID Number:	**0017387**
Date adjudicated by DHS Privacy Office:	June 14, 2024
PTA Expiration Date:	June 14, 2025

DESIGNATION

Privacy Sensitive System:	Yes
Category of System:	System 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:	**System covered by existing PIA** DHS/CBP/PIA-056 Traveler Verification Service
SORN:	**System covered by existing SORN** DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297; DHS/CBP-007 Border Crossing Information (BCI), December 13, 2016, 81 FR 89957; DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778; DHS/CBP-021 Arrival and Departure Information System (ADIS), November 18, 2015, 80 FR 72081

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)

(b)(5)