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/Planning, Program Analysis, and Evaluation**
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	**February 24, 2017**	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable):[1]	**Complete**	**Expected ATO/ATP/OA date (if applicable):**	**December 12, 2020**

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b) (6) (b) (7) (c)		
Office:	**CBP/OFO/APP/ Biometric Entry-Exit Strategic Transformation**	**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)

[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

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

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated 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 comparison technology, now known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. CBP previously issued Privacy Impact Assessments (PIA) documenting each new phase of TVS testing and deployment. In November 2018, CBP issued a comprehensive PIA, DHS/CBP/PIA-056, to a) consolidate all previously issued PIAs and b) provide notice to the public about how TVS collects and uses personally identifiable information (PII). CBP is in the process of updating the appendices of TVS PIA.

The last PTA was adjudicated on July 7, 2020 and expires on July 7, 2023. There are no major updates to this PTA since the last adjudication.

Background

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. CBP uses TVS as its backend matching service for all biometric entry and exit operations that use facial comparison, regardless of air, land, or sea.

Biometric Galleries

Regardless of the method of entry or exit, e.g., pedestrian, vehicle, cruise ship, vessel, or airplane, the TVS conducts the backend biometric matching and provides a result to different CBP systems depending on the environment. For all biometric matching deployments, the TVS relies on biometric templates generated from pre-existing photographs that CBP already maintains in other systems. 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 or exit. If CBP has access to advance passenger information or other advance arrival information, CBP builds galleries of photographs based on upcoming arrivals or departures. In instances where API or other advance passenger information does not exist, , TVS conducts a 1:1 service, which compares a live photo against a photo taken from the traveler's travel document.

CBP creates localized photographic galleries using either Advance Passenger Information System (APIS) data or against specific data sources (i.e., Trusted Traveler or advance arrival information received via CBP One that are within CBP holdings). To populate the localized galleries with photographs, CBP compiles photographs from existing CBP sources from the Passenger Systems Program Directorate (PSPD) Traveler Documentation and Encounter Data (TDED). 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.

CBP Collection Process at entry or exit
Due to the complexities in logistics across the entry and exit environments, CBP collects photographs of the arriving or departing traveler via several different iterations depending on the local port of entry. When the traveler presents him or herself for entry, or for exit, the traveler will encounter a camera connected to CBP's cloud-based TVS facial matching service via a secure, encrypted connection. The camera may be owned by CBP, the air or vessel carrier, another government agency (e.g., TSA), or an international partner.

Matching Process
The camera matches templates of the live images with existing photo templates from passenger travel documents. 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 TVS, templates cannot be reverse engineered to recreate a biometric image. Once the camera captures a quality image and the system successfully matches it with historical photo templates of all travelers from the gallery associated with that particular manifest, the traveler proceeds to inspection for admissibility by a CBP Officer or exits the United States. 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 (e.g., comparing the traveler to their travel document photo) by either CBP, TSA, or the gate agent, depending on the environment.

As recommended by the National Institute of Standards and Technology (NIST), CBP's Biometric Air Exit Key Performance Parameters mandate that the system's True Acceptance Rate (TAR) must equal or exceed 97 percent of all in-scope travelers and that the system's False Acceptance Rate (FAR) must not exceed 0.1 percent of all in-scope travelers. If it is seen that the TAR or FAR is falling below acceptable rates, then adjustments to the matching threshold can be made. This involves a process of re-analyzing the ground truthed data and developing new recommended thresholds with supporting data.

Retention and Storage
With the operational deployment of TVS, CBP transmits facial images for in-scope travelers[2] 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

[2]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.

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 comparison process. For U.S. citizens who do not out opt out, CBP retains the image for no longer than 12 hours as well as a 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 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.

Additional use cases
In addition to using TVS as the backend matching service for all biometric entry and exit operations, CBP also uses TVS as a facial comparison tool in support of other CBP mission related purposes. For example, CBP is deploying the ESTA mobile application where CBP will collect a "selfie" from the ESTA applicant as well as their passport photograph from the biographic passport data page. ESTA interfaces with TVS to compare the two photographs to conduct a 1:1 match with the "selfie" and passport photograph to biometrically verify the applicant's identity. If the two photographs are a match, TVS will send a match response back to ESTA. In the rare event that TVS is unable to match the "selfie" to the passport photograph, the mobile application will prompt the applicant to retake a "selfie." An applicant can attempt to retake the selfie up to three times. Another example, as part of the secondary inspection for the ATA process, the CBP officer may use the 1:1 photo comparison tool within Unified Secondary (USEC) to compare the previously submitted CBP One™ photo to the photo from primary processing. USEC sends the CBP One™ and Simplified Arrival photograph to TVS who then responds with a match score on a scale of 0-10000. This photo comparison is a tool for officers to help determine if the noncitizen who submitted the ATA application is the same noncitizen who arrived at the POE. CBP completes separate PTAs to document uses cases that support CBP beyond biometric entry and exit operations.

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) are 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[3] ☒ 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)[4] ☐ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

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

Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individual or population.

CBP collects facial images as well as personal information from the APIS manifest, which is already being collected by the airlines. 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).

[3] 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.

[4] 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*

(b)(7)(E)

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

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?[5] 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.[6] *Please list modalities (e.g., fingerprints, DNA, iris scans): Click here to enter text.* ☐ 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*,[7] 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*

[5] 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.

[6] 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.

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

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.[8] 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.*[9]	CBP temporarily retains facial images of non-immigrants and lawful permanent residents 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 of hours. Photos of in-scope travelers are retained in IDENT for up to 75 years, consistent with existing CBP records that are housed in IDENT in accordance with the BCI SORN. CBP continues to work with NARA to develop the appropriate retention schedule. CBP Records and Information Management (RIM) Office advised that a NARA-approved retention schedule was only

[8] 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.

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

	required for U.S. citizen photos. CBP is currently updating the required forms before resubmitting them to NARA for approval.
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?[10]	☐ 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 in order 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 partners with NIST to test technologies developed by specified vendors and to evaluate algorithms on biometric projects. Currently, NIST provides a positive/negative result after the matching analysis.
8. Is this sharing pursuant to new or existing information sharing agreement	N/A

[10] 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.

(MOU, MOA, LOI, RTA, etc.)? *If applicable, please provide agreement as an attachment.*	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 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[11] ☐ Live PII data for testing ☒ No

[11] 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)?[12] 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: CBP has an IAA with NIST to conduct a comprehensive study/analysis of CBP's utilization of facial comparison technologies in biometrics entry/exit programs.

12. Does the planned effort include any interaction or intervention with human subjects[13] 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.[14]

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.*

[12] 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.

[13] 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.

[14] 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?[15]	☐ 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

[15] 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:	**May 16, 2023**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	June 13, 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):	(b) (6)
Workflow Number:	**0014673**
Date approved by DHS Privacy Office:	June 15, 2023
PTA Expiration Date	June 15, 2024

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)