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:	**Simplified Arrival – Bus Manifest**		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	Office of Field Operations (OFO)/Planning, Program Analysis and Evaluation (PPAE)
FISMA Name (if applicable):	Simplified Arrival	**FISMA Number (if applicable):**	CBP-07779-SUB-00024
Type of Project or Program:	System	**Project or program status:**	Operational
Date first developed:	**April 18, 2023**	**Pilot launch date:**	N/A
Date of last PTA update	September 25, 2017	**Pilot end date:**	N/A
ATO Status (if applicable):[1]	**Complete**	**Expected ATO/ATP/OA date (if applicable):**	**December 8, 2023**

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b) (6), (b) (7)(C)		
Office:	**OFO/PPAE**	**Title:**	Program Manager, Pedestrian Processing
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)@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: Updated PTA

CBP is submitting this PTA to document enhancements of Simplified Arrival to include the manifest process concept in the land border pedestrian ports of entry.

The Simplified Arrival entry solution leverages biometrics to initiate a transaction, using facial comparison as the primary identity verification method. Historically, travel documents such as passports or visas are used to verify a traveler's identity, review travel history, and highlight any enforcement concerns that may require attention, prior to admission to the United States. This shift from a biographic, document-based system to biometrically initiated transactions, requires travelers to provide facial biometrics for identity verification purposes.

Voluntary Bus APIS

Under 19 U.S.C. 1431(b), CBP has the authority to collect manifest data from vessels, aircraft, or vehicles entering the United States. In addition to the mandatory submissions provided by both commercial air and vessel carriers and private aircraft pilots, CBP receives voluntary Advance Passenger Information System (APIS) submissions from rail and bus carriers. Private and commercial rail and bus carriers can submit passenger and crew manifests to CBP via direct system connections, through the Electronic Advance Passenger Information System (eAPIS) web interface, or through the CBP One app. This information is submitted by the carrier directly or by a third-party contractor hired on behalf of the carrier to gather and submit passenger information. While both bus and rail carriers and operators can submit voluntary APIS, this PTA is limited to bus carrier operators only.

API contains information collected by bus carriers, including biographic data, document information, details about the traveler's itinerary, such as bus number and carrier name. API is screened against TECS records and other law enforcement databases, allowing CBP to ascertain, pre-arrival, if any security or law enforcement risks exist.

Existing Bus Pedestrian Processing

Currently, all arriving bus passengers are processed the same way arriving pedestrians. A bus traveler will get off the bus and queue in a designated area of the POE. When the bus traveler approaches a primary officer, he or she will present their travel document. The officer will take a photo of the traveler and query the travel document. Simplified Arrival transmits the live photo and document information to the Traveler Verification Service (TVS) for a 1:1 match. The 1:1 match verifies the traveler's identity (new photo taken at primary) against the source photo associated with the document. Simplified Arrival returns the result (match or no match), as well as the personal information returned from the document query (including any derogatory information). The officer then proceeds with the inspection, and either admits the traveler into the United States or refers the traveler to secondary processing.

New Bus Pedestrian Processing

When a bus operator or carrier voluntarily submits a manifest, TVS will build a photo gallery of individuals on the manifest in advance of the bus arriving at the port of entry. TVS will assemble the photo gallery from DHS holdings, to include photographs from the Travel Document Encounter Database (TDED).

Upon arrival, all bus travelers will proceed to the entry lanes within CBP's Federal Inspection Services (FIS); their picture will be taken, either automatically by a camera at the booth, or by the primary officer. Simplified Arrival will transmit the image to TVS, which creates a template from the image and uses the template to query against the pre-assembled gallery of known identities, based on the bus manifests for incoming buses that day.

Once the traveler is matched, TVS will transmit the match results to Simplified Arrival. In turn, Simplified Arrival will retrieve the traveler's biographic information. The primary officer will have the ability to view and evaluate the traveler's biographic data, along with derogatory information, and the associated match result in Simplified Arrival.

Upon admission, the traveler's crossing history is updated in the Arrival Departure Information System (ADIS) to reflect a confirmed arrival into the United States with manifest information. Consistent with the existing process for non-U.S. citizens, the traveler's biometric information is recorded in the Automated Biometric Identification System (IDENT), will be updated to reflect a biometrically confirmed arrival into the United States.

Through TVS, CBP transmits facial images for in-scope travelers 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. Since 2004, CBP has collected biometric information in the form of fingerprints and a facial photo on entry for in-scope travelers; CBP transmits this information to IDENT, where it is stored in association with a Fingerprint Identification Number (FIN). Each FIN is associated with individual encounters (EID), which represent each interaction between that individual and an IDENT data provider. These encounters include the face image, full name, and gender. CBP does not store facial images voluntarily collected from U.S. citizens in IDENT, as U.S. citizens are not considered in-scope. CBP does not retain images of U.S. citizens once their identities are verified by TVS. Only photos of non-U.S. citizens are retained for the full 14 days in ATS-UPAX and for the full retention period in IDENT. In addition, within 12 hours, CBP purges all photos, regardless of immigration or citizenship status, from the TVS cloud matching service. Retention is described in detail in section 5 of the TVS PIA.

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[2] ☒ Members of the public

[2] 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.

	☒ 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)[3] ☒ Refugees/Asylees ☒ Other. All travelers who enter the United States.

3. What specific information about individuals is collected, maintained, used, or disseminated?
The information to be retrieved and associated with a traveler from DHS systems and/or collected from travelers, includes complete name, date of birth, gender, country of citizenship, passport number and country of issuance, country of residence, travel document type (e.g., visa), number, issue date, expiration and country of issuance, class of admission, crossing information, fingerprint identification number, facial photographs, and digital fingerprint scans. This is very similar to the current primary entry process except that photographs will be taken for all travelers. **CBP will not retain U.S. citizen photos under this initiative.**
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?[4] If applicable, check all that apply.

[3] 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)

[4] 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.

☐ 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
Biometric identifiers *(e.g., FIN, EID)*
☒ Biometrics.[5] *Please list modalities (e.g., fingerprints, DNA, iris scans):* **Facial image**
☐ 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*,[6] 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.[7] Please list all unique identifiers used: • **TVS:** Facial image template • **Simplified Arrival**: TECS system-generated unique traveler identifier (not linkable outside of TECS), or biographic information.

[5] 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 accomplishedIDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

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

[7] 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.

	• **ATS/UPAX**: UPAX-generated unique photo identifier (not linkable outside of ATS/UPAX or TPAC) ☐ 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.*[8]	CBP is working with NARA to develop the appropriate retention schedule.
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)?	CBP documents the deletion of U.S. Citizens photographs. CBP monitors when photos are accessed and/or used in CBP's facial matching service. Furthermore, deletion of U.S. citizen photographs is verified during routine data analysis. Additionally, CBP audits periodically to ensure adherence to the retention policy.

6. **Does this Project, Program, or System connect, receive, or share PII with any other DHS/Component projects, programs, or systems?**[9]	☐ No. ☒ Yes. If yes, please list: • TECS/Simplified Arrival • Advance Passenger Information System (APIS) • DHS Office of Biometric Identity Management (OBIM) – IDENT belongs to OBIM • Automated Biometric Identification System (IDENT). • Traveler Verification Service (TVS)
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:

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

[9] 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.

	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: N/A
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: ☐ Yes. In what format is the accounting maintained: *Click here to enter text.*

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

[10] 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)?[11] 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[12] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for <u>research purposes</u>	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for <u>independent</u> review and approval of this effort.[13]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, <u>in addition</u> to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: New primary processing training is provided to CBPO users. Role-based training is available for ISSO's, System Owner's and system administrators.

[11] 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.

[12] 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.

[13] 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?[14]	□ 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] 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:	***March 9, 2023***
Concurrence from other Component Reviewers involved (if applicable):	*Click here to enter text.*
Date submitted to DHS Privacy Office:	*March 10, 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 a date.*
Workflow Number:	***0024084***
Date approved by DHS Privacy Office:	*March 10, 2023*
PTA Expiration Date	*March 10, 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:	**New PIA is required.** DHS/CBP/PIA-056 Traveler Verification Service **[appendix update required]**; Simplified Arrival PIA **[forthcoming]**; DHS/CBP/PIA-001 Advance Passenger Information System (APIS); DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative
SORN:	**System covered by existing SORN** DHS/CBP-005 Advance Passenger Information System (APIS), March 13, 2015, 80 FR 13407; 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 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)