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:	**Simplified Arrival (TECS Subsystem)**		
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 (TECS CLOUD)**	**FISMA Number (if applicable):**	**CBP-07779-SUB-00024**
Type of Project or Program:	**System**	**Project or program status:**	**Operational**
Date first developed:	Click here to enter a date.	**Pilot launch date:**	**N/A**
Date of last PTA update	**May 19, 2020**	**Pilot end date:**	**N/A**
ATO Status (if applicable):[1]	**Not started**	**Expected ATO/ATP/OA date (if applicable):**	Click here to enter a date.

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b) (6) (b) (7) (c)		
Office:	**PSPD**	**Title:**	Program Manager
Phone:	(b) (6) (b) (7) (c)	**Email:**	(b) (6) (b) (7) (c)

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) @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

Simplified Arrival is a CBP Major Application for primary processing of passengers at Ports of Entry that resides within the CBP Amazon Cloud Environment (CACE). Facial biometrics are deeply integrated into the Simplified Arrival workflow to reduce passenger processing time. CBP previously had separate PTAs to cover the different uses of Simplified Arrival depending on a traveler's mode of entry. This PTA combines all Simplified Arrival (SA) uses cases into one SA PTA. SAMN is the acronym used for the code deployment for SA-Air Sea. SAPN is the acronym used for the code deployment for SA-Ped. SA provides advanced facial comparison biometric technologies which provides significant facilitation benefits while increasing security and enforcement.

Simplified Arrival:

In 2017, CBP deployed Simplified Arrival (SA), which uses a traveler's newly captured photograph to initiate a facial comparison transaction as the principal identity verification. This shift from a biographically, document-based system to biometrically initiated transactions through SA, enhances CBP's ability to facilitate lawful travel and secure the border. The biometric facial comparison process occurs only at a time and place where travelers are already required by law to verify their identity when presenting themselves for inspection at a United States (U.S.) port of entry.

As a traveler arrives at an air, land, or seaport of entry, the traveler pauses for a photograph at the primary inspection point. SA then performs systems queries against the pre-staged manifest galleries to match the traveler and their "probe" photograph to the traveler's "source" photographs in DHS holdings in the gallery.

If SA confirms a match, the CBP officer completes the remaining steps in the primary inspection process and admits the traveler or refers the traveler for a secondary inspection. If a traveler cannot be matched to a photograph in DHS holdings, using the Traveler Verification Service (TVS), a document scan is attempted which allows for the passport chip to be opened and the biographic data retrieved.

CBP uses the TVS as its backend matching service for all biometric entry (and exit) operations that use facial comparison, regardless of whether the individual travels by air, land, or sea. CBP has implemented various SA use cases to enhance the arrival process for international travelers. Though the facial comparison encounter modality may differ, SA performs the same system checks and identity verification using TVS to compare a traveler's face to their travel document (e.g., passport). These use cases are described below.

Opt-out

U.S. citizens are not required to provide biometrics as part of the entry process and may choose to opt-out of the biometric collection process. Privacy signage is posted at CBP ports of entry, either through electronic LED messaging board or posted signage. The signage is visible for the traveler to read prior to encountering a CBP officer to begin the SA process. U.S. citizen travelers that choose to opt-out, notify the CBP officer of their choice to opt-out as they approach the primary inspection point. The CBP officer then processes the traveler through the traditional inspection process consistent with existing requirements for admission into the United States. In addition to U.S. citizens having the opportunity to opt-out, there are certain non-U.S. citizens that may also opt-out of the biometric capture taken as part of the SA process.

This group includes travelers under the age of 14 and over the age of 79, diplomats, Canadians, and otherwise exempt nonimmigrants. However, CBP is drafting a regulation requiring all noncitizens to submit to biometric collection by CBP at entry and exit. The Notice of Proposed Rulemaking is currently under review by DHS Office of General Counsel.

Simplified Arrival Air:
In the fall 2017, CBP began a biometric primary entry process, using commercial off-the-shelf cameras, Traveler Primary Arrival Client (TPAC), a subsystem of TECS and the Traveler Verification Service (TVS); to capture facial biometric data from all travelers entering the United States. All information that was collected, and generated, was retained in TPAC. This upgraded technical program was called TPAC-FACE. TPAC-FACE was implemented as an interim solution while SA was being developed and was phased out as SA was deployed.
The entry process closely follows the processes outlined in the TECS System: CBP Primary and Secondary Processing PIA (December 22, 2010)[2]. CBP obtains biographic information from the Advanced Passenger Information System (APIS) manifest on travelers boarding international flights. The manifest includes specific details of the traveler's itinerary, such as flight number, carrier, originating airport, and destination airport. The information transmitted to CBP through APIS also includes biographic information such as the traveler's full name, date of birth, country of citizenship, passport information, and a unique identifier (UID) which is a numeric or alphanumeric string that is associated with a single entity within a given system CBP screens the APIS information against TECS records and other law enforcement databases for CBP to ascertain if any security or law enforcement risks exist. CBP then builds a "gallery" of "source" photographs to create a biometric template. TVS utilizes biographic information received from APIS transmissions to then query DHS holdings to retrieve or pull photographs. Once the photograph is "pulled", it is templatized and placed into a gallery for matching.
Arriving travelers proceed to the entry lanes within CBP's Federal Inspection Services (FIS), and a CBP officer takes a photograph of the traveler at the primary booth. CBP's SA system transmits the image to TVS. To biometrically identify the traveler, TVS automatically creates a template from the image and uses the template to query against a gallery of known identities based on the manifests for all incoming flights for that day, based on the APIS manifests that already exist within DHS systems for that day. Once the traveler is matched by TVS, the CBP officer conducts the inspection and establishes the purpose and intent of travel.

In case of a facial no-match, the CBP officer scans the traveler's document. The system then compares the live captured image with the photograph on the document's e-chip; this process is referred to as 1:1 verification.

If the eligible traveler requests to opt-out, the CBP officer scans the traveler's document.

The "gallery" photographs are deleted from the TVS cloud based on business rules such as six (6) hours after arrival for air entry but no later than 12 hours. The no-later-than 12 hours for gallery photograph

[2] See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates), and U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), available at https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

deletion is built in for CBP's safeguard in the event there is a system error or delay in processing air arrival travelers (system outage, weather delays, canceled flights, etc.) CBP deletes the live encounter facial images (photographs) of biometrically verified U.S. citizens collected through this process within 12 hours. If the TVS cloud matching service determines that a particular traveler is a U.S. citizen, CBP immediately bypasses photograph storage; the photograph of the U.S. citizen is not retained. CBP retains facial images of non-U.S. citizens and lawful permanent residents for no more than 14 days in TVS for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.

Simplified Arrival - Sea

In 2021, CBP deployed SA Sea to modernize the arrival process in the cruise environment by using facial comparison technology. The entry process for cruise line passengers and crew members mirrors SA for Air arrivals and begins with a facial photograph capture rather than a document scan. SA Sea is used to process arriving passengers and crew members on open loop cruises.[3] SA Sea, like SA Air, uses the APIS manifest and CBP creates a gallery of historical photograph templates from DHS holdings. Cruise line passengers debark the vessel and the CBP officer takes a photograph of the traveler during the primary encounter. Once the traveler is matched by the TVS, the CBP officer conducts the standard inspection interview and establishes the purpose and intent of travel. In case of a no match, the CBP officer scans the traveler's document. The system then compares the live photograph with the photograph on the document's e-chip; this process is referred to as 1:1 verification. After the traveler's identity is confirmed, the CBP officer determines admissibility, and either refers the traveler to secondary processing for further inspection or directs the traveler to proceed. U.S. citizens and those eligible non-citizens that do not wish to have their photograph taken, can opt-out and request manual identity verification.

The "gallery" photographs are deleted from the TVS cloud based on business rules such as 12 hours after arrival for sea entry but no later than 12 hours. The no-later-than 12 hours for gallery photograph deletion is built in for CBP's safeguard in the event there is a system error or delay in processing sea arrival travelers (system outage, weather delays, etc).

CBP deletes the live encounter facial images of biometrically verified U.S. citizens collected through this process within 12 hours. If the TVS cloud matching service determines that a particular traveler is a U.S. citizen, CBP immediately bypasses photograph storage; the photograph of the U.S. citizen is not retained. CBP retains facial images of non-U.S. citizens and lawful permanent residents for no more than 14 days in TVS for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.

Simplified Arrival – Land

*Pedestrian***:**

Utilizing SA- Pedestrian, the CBP officer takes a photograph of the traveler and queries the travel document. SA transmits the live photograph and document information, when available, to the TVS for a 1:1 match. The 1:1 match verifies the traveler's identity (live photograph taken at primary) against the source photograph associated with the document. In the case of undocumented individuals who submitted advance information via CBP One, TVS matches the live photograph against a gallery of CBP One photographs. SA returns the result (match or no match), as well as the personal information returned from the document

[3] Open loop refers to voyages that arrive at a U.S. Port of Entry from a foreign port of call outside the scope of closed loop definitions. This includes cruises which originated in a foreign port, as well as voyages which started in a U.S. port but touch a port of call outside the definition of closed loop.

query, including any derogatory information. The CBP officer then proceeds with the inspection, and either admits the traveler into the United States or refers the traveler to secondary for further processing.

Bus/Rail

CBP processes pedestrians and bus passengers in a similar manner. When a pedestrian or bus traveler approaches a primary officer, he or she presents their travel document. The officer takes a photograph of the traveler and queries the travel document. SA transmits the live photograph and document information to TVS for a 1:1 match. The 1:1 match verifies the traveler's identity (new photograph taken at primary) against the source photograph associated with the document. SA returns the result (match or no match), as well as the personal information returned from the document query (including any derogatory information). The CBP officer then proceeds with the inspection, and either admits the traveler into the United States or refers the traveler to secondary processing. When a bus operator or carrier voluntarily submits a manifest, TVS builds a photograph gallery of individuals and travelers approach primary where TVS performs a 1:n match with the manifest gallery. The "gallery" photographs are deleted from the TVS cloud based on business rules such as six (6) hours after arrival for bus/rail entry (with manifest) but no later than 12 hours. The no-later-than 12 hours for gallery photograph deletion is built in for CBP's safeguard in the event there is a system error or delay in processing bus/rail arrival travelers (system outage, weather delays, etc).
CBP deletes the live encounter facial images of biometrically verified U.S. citizens collected through this process within 12 hours. If the TVS cloud matching service determines that a particular traveler is a U.S. citizen, CBP immediately bypasses photograph storage; the photograph of the U.S. citizen is not retained. CBP retains facial images of non-U.S. citizens and lawful permanent residents for no more than 14 days in TVS for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.

Vehicle

As part of the standard land border inspection process, vehicles are presented to CBP at the vehicle primary border crossing lanes upon arrival at a port of entry. SA-Vehicle links travelers with a vehicle in a single package for the CBP officer to process.
CBP employs Radio Frequency Identification (RFID) and License Plate Reader (LPR) technology in vehicle crossings to capture and collect data in accordance with the RFID and LPR PIAs. Cross border travel documents contain unique numbers embedded in RFID tags. Upon arrival in a vehicle crossing lane, the unique number is read wirelessly by the RFID technology and then forwarded through a secured data circuit to the vehicle package. Simultaneously, the LPR technology captures license plate information. The RFID and LPR data are packaged and transmitted to SA-Vehicle. A standard vehicle package includes the following: License Plate Reader images (Front, back, and scene images of the tag); the Optical Character Recognition (OCR) translation of the plate of the inbound vehicle; the travelers' biographic information (name, DOB, nationality, and class of admission); and message ID.
SA-Vehicle uses the unique RFID number to retrieve personally identifiable information about each traveler and presents the information to the primary CBP officer. The CBP officer uses the information to authenticate the identity of the traveler and to facilitate the land border primary inspection process. At vehicle primary, the CBP officer may obtain information directly from the driver and traveler(s) within the vehicle via their travel documents if they were not transmitted via RFID.
SA – Vehicle has an adjudicated PTA on file.

Fingerprint collection (if applicable)

After transmission to IDENT, IDENT returns a response to Simplified Arrival to indicate whether the CBP officer is requested to obtain fingerprints from the traveler. CBP typically only collects fingerprints from first-time non-U.S. citizen travelers or those who cannot be biometrically verified through the Simplified Arrival facial image. CBP collects the fingerprints from the traveler as CBP deems appropriate and IDENT enrolls the fingerprints into IDENT upon receipt and either stores the photograph with an existing Fingerprint Identification Number (FIN) or generates a new FIN.

Biometric (Facial Recognition) Vetting/Screening

Once the traveler is matched, TVS transmits the match results, along with a TECS system-generated unique traveler identifier to retrieve the traveler's biographic information from the APIS manifest. Additionally, SA uses the TVS-generated identifier to retrieve the source photograph which is compared to the live photograph taken during the primary encounter to attempt the biometric confirmation. The CBP officer has the ability to view and evaluate the traveler's biographic data, along with any potential derogatory information (i.e. Terrorist Screening Database (TSDB), TECS Lookout Records, DHS Biometric Identity Management System (IDENT)/the Homeland Advanced Recognition Technology System (HART), Watchlist records, as well as data concerning outstanding wants and warrants) in SA along with associated biometric match results from TVS. The CBP officer conducts an interview to establish the purpose and intent of travel. Once the CBP officer determines admissibility, the CBP officer refers the traveler to secondary for further inspection or releases the traveler. Upon admission, the traveler crossing history is updated in the TECS System to reflect a confirmed arrival into the United States. Consistent with the existing process for in-scope non-U.S. citizens, the DHS Office of Biometric Identity Management (OBIM), Automated Biometric Identification System (IDENT) crossing history is updated to reflect a biometrically confirmed arrival into the United States.

In case of a facial no-match, the CBP officer scans the traveler's document. The system then compares the live photograph with the photograph on the document's e-chip; this process is referred to as 1:1 verification.

Retention/Storage

Photographs of non-U.S. citizens are enrolled in the Automated Biometrics Identification System (IDENT)/ Homeland Advanced Recognition Technology System (HART), as a biometric confirmation of arrival. CBP retains biographic entry (and exit) records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-U.S. citizens, consistent with the Border Crossing Information (BCI) System of Records Notice (SORN). In addition, CBP maintains entry and exit records in the Arrival and Departure Information System (ADIS) for lawful permanent residents and non-U.S. citizens, consistent with the ADIS SORN. Finally, records retained in association with a law enforcement action are retained for 75 years, consistent with the TECS SORN. Pursuant to 8 U.S.C. § 1365b; 8 C.F.R. 235.1(f)(1)(ii) photographs for certain non-U.S. citizens are retained in secure Department of Homeland Security systems and used as a biometric confirmation of arrival (and departure) into (and out of) the U.S.

CBP retains facial images of non-U.S. citizens and lawful permanent residents for no more than 14 days in TVS for confirmation of travelers' identities, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.

All templatized photographs may remain in the cloud for no longer than 12 hours. Once the TVS cloud matching service determines that a particular traveler is a U.S. citizen, CBP immediately bypasses photograph storage, and the photograph is not retained. If, however, the traveler presents him/herself as a

citizen of another country, the photograph is processed and retained accordingly. All templatized photographs remain in the cloud for no longer than 12 hours.

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] ☒ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

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, date and country of issuance, crossing information, fingerprint identification number, A-number, driver's license #, facial photographs, and digital fingerprint scans.

[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 Directive 002-02, Implementation of Section 1367 Information Provisions, *available at*

(b)(7)(E)

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):* **fingerprints and facial photographs** ☐ 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*,[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:

[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.

[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.

	Alien Number (A-Number), Visa Number, Passport Number, Driver's License/ State ID Number, Biometrics ☐ By a non-unique identifier or other means. Please describe: This ID is generated when the initial document data and is sent to the backend TECS. Stored in TECS for that encounter, along with the document details

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]	CBP is in the process of working with NARA to formalize a retention schedule. 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 that are not matched and are confirmed to be non-citizens are retained for no longer than 14 days after match/no-match. Finally, CBP images of in-scope travelers are shared with IDENT and stored in accordance with the IDENT retention schedule, DAA-0563-2013-0001-0006. SA audit logs including traveler crossing information along with the officer action that was performed during the primary inspection are retained for 6 years. CBP retains biographic entry records for 15 years for U.S. citizens and lawful permanent residents and 75 years for non-citizens. CBP is working to formalize the retention period for border crossing information.
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)?	. TVS automatically deletes the photograph once the retention criteria has been met. CBP has not deleted any crossing information until the retention schedule has been completed.

6. Does this Project, Program, or System connect, receive, or share PII with any	☐ No.

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

other DHS/Component projects, programs, or systems?[11]	☒ Yes. If yes, please list: DHS Office of Biometric Identity Management (OBIM)
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.*	N/A 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: *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[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)	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

[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.
[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.

(i.e., data mining)?[13] This does not include subject-based searches.	
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[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: **New primary processing training is provided to CBPO users. Role-based training is available for ISSO's, System Owner's and system administrators.**

14. Is there a FIPS 199 determination?[16]	☐ No. ☒ Yes. Please indicate the determinations for each of the following:

[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.

[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.

	Confidentiality: ☐ Low ☒ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☒ Moderate ☐ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b) (6) (b) (7) (c)
PRIVCATS ID Number:	**0016310**
Date submitted to Component Privacy Office:	Click here to enter a date.
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	January 31, 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):	(b) (6)
PRIVCATS ID Number:	**0016310**
Date adjudicated by DHS Privacy Office:	March 4, 2024
PTA Expiration Date:	March 4, 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:	**New PIA is required.** DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative; CBP Simplified Arrival PIA **[forthcoming]**
SORN:	**System covered by existing SORN** DHS/CBP-007 Border Crossing Information (BCI), December 13, 2016, 81 FR 89957; 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)