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:	**Trusted Traveler Program**		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	Office of Field Operations
FISMA Name (if applicable):	**Trusted Traveler Program (TTP)**	**FISMA Number (if applicable):**	**CBP-07684-MAJ-07684**
Type of Project or Program:	**Program**	**Project or program status:**	**Operational**
Date first developed:	**October 14, 2011**	**Pilot launch date:**	**N/A**
Date of last PTA update	**November 18, 2020**	**Pilot end date:**	**N/A**
ATO Status (if applicable):[1]	**Complete**	**Expected ATO/ATP/OA date (if applicable):**	Click here to enter a date.

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b) (6), (b) (7)(C)		
Office:	CBP/OFO	**Title:**	Supervisory CBPO
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

Purpose. The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) submits this PTA for the Trusted Traveler Program (TTP Program) as a renewal PTA and to account for updates since the last PTA. This PTA addresses the following:

- As a renewal PTA, this PTA renews PTA, CBP - TTP Program, dated 20201118 which expires this November.
- As an update PTA, this PTA more accurately describes the TTP application process and includes changes to the enrollment process for minors.

Background

DHS has a mission to secure the nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. By law, all persons arriving at a port of entry to the United States are subject to inspection by a CBP Officer. CBP uses business processes and technologies that allow CBP to optimize limited officer resources, facilitate traveler entry processing, and reduce wait times, while continuing to enforce customs and immigration laws.

DHS created the Trusted Traveler Programs, a group of distinct services, also known as programs, for individuals who enroll as program members after allowing CBP to determine that the individuals meet the programs' eligibility criteria. The TTPs' individual services expedite the travel of pre-approved low-risk travelers arriving in the United States utilizing facial recognition portals at airports (and in certain circumstances, mobile applications), dedicated lanes at land border ports of entry, and expedited processing at maritime reporting locations, and allowing CBP to focus its limited resources on higher risk unknown travelers.

This PTA covers the CBP TTP services for international travelers, described below. As indicated, travelers apply and become members of individual TTP programs after submitting an application then undergoing initial and recurrent vetting processes as well as an enrollment interview, all through which CBP collects, maintains, uses, and disseminates personally identifiable information (PII).

- **Global Entry,** available at designated airports, expedites the entry processing of pre-approved international, low-risk members. Global Entry program members are validated through the use of facial recognition portals, as well as through the new Global Entry Mobile App currently piloted at several select airports.
- **SENTRI** provides expedited entry processing of pre-approved low-risk travelers arriving in the U.S. by land at southern border ports of entry.
- **NEXUS** is a bi-national TTP operated jointly by the U.S. and Canada. NEXUS provides expedited CBP and Canada Border Services Agency (CBSA) processing for travelers entering both the U.S. and Canada via the air, land, or marine environments. Program members use dedicated processing lanes at designated northern border ports of entry, NEXUS kiosks when entering Canada by air and Global Entry portals when entering the United States via Canadian Preclearance airports. NEXUS members also receive expedited processing at designated marine reporting locations.

- **FAST** allows expedited processing for commercial drivers who have completed background checks and fulfill certain eligibility requirements. FAST enrollment is open to commercial drivers from the United States, Canada, and Mexico. FAST participants utilize designated lanes at land border ports of entry which process commercial cargo.
- **U.S. APEC Business Travel Card Program** is a voluntary program to facilitate travel for U.S. citizens engaged in verified business in the APEC region and U.S. government officials engaged in APEC business. The U.S. APEC Business Travel Card will enable access to fast-track immigration lanes at airports in foreign APEC member economies. Participants must also be an existing good standing member of a CBP trusted traveler program. This Program is currently listed with PRIVCATS ID 0012967 which can now be retired.

TTP applicants fill out an application online and pay their processing fee. TTP Program applicants can use TTP Online, a cloud-based web application, or in the future, a new TTP Mobile application on the CBP One™ Mobile Application to provide the necessary information. TTP Mobile is the subject of a separate upcoming PTA. CBP uses Login.gov to authenticate TTP users.

Applicants create a TTP account and provide their biographic information (name, date of birth, city and country of birth, and email address) to associate their Login.gov account to their TTP profile. Registered TTP users are then allowed to select their desired Trusted Traveler Programs and provide the required information to apply. Program members may make limited updates to their data through the online TTP dashboard once their application reaches a certain status. Applicants also may monitor their application and enrollment status online. To pay any applicable fees, the TTP System directs TTP users to Pay.gov.

CBP uses the biographic information submitted as part of the application to conduct vetting against selected security and law enforcement databases at DHS, including TECS and the Automated Targeting System (ATS)). In addition, the NTC conducts enhanced vetting against classified holdings including National Counterterrorism Center (NCTC) holdings. Using this information, ATS builds a risk assessment. ATS risk assessments are always based on predicated and contextual information. ATS traveler risk assessments do not use a score to determine an individual's risk level; instead, they compare personally identifiable information (PII) against system-identified potential matches to derogatory information.

After CBP reviews the application and completes the necessary vetting, CBP will either conditionally approve the application or deny it. If the applicant is conditionally approved, CBP sends the applicant an email notification indicating that a status in their application has changed to instructs the applicant to login to their TTP dashboard. The conditional approval letter contains the applicants PASSID/membership ID. Upon logging in to TTP, the applicant is presented with instructions on how to schedule an interview with CBP. These interviews typically occur at an enrollment center. However, Global Entry applicants may also complete interviews at a port of entry upon returning from an international flight at an Enrollment on Arrival designated airport and NEXUS applicants may complete enrollment at CBP Pre Clearance locations once the CBSA interview is completed.

As part of the interview process and background vetting, CBPOs collect the applicant's fingerprints and photograph. TTP submits this information to the CBP IXM biometrics service. IXM interfaces with IDENT/Homeland Advanced Recognition Technology (HART) used by the Office of Biometric Identity Management (OBIM) for vetting and enrollment. If an individual supplies their fingerprints as part of the

Enrollment on Arrival process, Simplified Arrival captures the fingerprints and sends them to TTP. TTP displays those prints to the Officer until the Officer chooses to send the prints for vetting. TTP stores those prints for 48 hours. Additionally, TTP sends a message to IDENT/HART via IXM with the fingerprints, however, this is not an accessible field in TTP. That is, no regular user will be able to access the fingerprints collected.

Typically, an application can be approved within 1-2 business days after the interview. There may be situations where additional information is required, such as submission of court documents, which may delay the approval of an application. Once approved, program members must activate their Trusted Traveler cards online. **TTP System Updates**

TTP Information Technology System

In the past, CBP used the Global Enrollment System-Trusted Traveler (GES-TT) as the main system to support the TTP Program. *See* PTA, CBP Global Enrollment Programs (GEP), dated August 14, 2023. Now, the TTP Program uses the TTP System, and plans to phase out GES-TT. *See* PTA, CBP - Trusted Traveler Program, dated July 20, 2020. The initial TTP System served as the primary public-facing online interface for applicants to submit the TTP application and make limited updates to their data. *See* DHS/CBP/PIA-002(d) Global Enrollment System, August 15, 2017. TTP Program data is currently stored within the Global Enrollment System security boundary. Over time, the TTP database, an Oracle database, will migrate to the TTP System security boundary.

GES-TT System Functionality Migration to TTP Internal

Currently, CBP is migrating the GES-TT system functions and capabilities to the TTP System's internal-facing interface, TTP Internal. Members of the public have no access to TTP Internal. CBPOs are the primary users.

TTP Internal provides CBP with the ability to centralize many of the application and enrollment functions from GES-TT. TTP Internal allows for standardization of the internal membership management capabilities and risk assessment processes. Overall, TTP Internal offers a more efficient approach in the administration of the TTP programs.

The migration of the GES-TT functions to TTP Internal is the update. For example, where a CBPO used the GES interface to submit data collected during the enrollment interview process along with the CBPO's adjudication, the CBPO will now use the TTP Internal interface.

Program Updates – Minor Enrollment Process Updates

Through this voluntary alternate enrollment procedure, TTP applicants who wish to submit their minor children (child 13 and under) as dependents attached to their TTP membership, would be able to associate their child(ren) to their Pass ID in the application process or after the parent's/guardian's initial approval. For the purpose of this section, the terms "minor child", "child" and "dependent" are interchangeable depending on grammatical context and all equate to a minor child age 13 and under.

Instead of creating a separate application for each child as is the current process, CBP's intent is to utilize existing application methodology and vetting procedure currently in place for vehicle enrollments. A parent/guardian would be able to add each child to their account as they would add a vehicle, either in an initial application or after approval. Each dependent would be issued their own Pass ID linked to the

parent's/guardian's "master" account. A cap on the number of dependents, as there currently is on vehicle additions, would not be placed on minor dependents. Children would be separated from the parents' membership, or "auto expired", once they reach 14 years of age, at which time they would need to submit an individual application and be subject to mandatory biometric collection.

In order to be eligible for auto-approval as a dependent, one of the following conditions must be met:

1. A new parent/guardian initial applicant obtains conditional approval, has added the child(ren) as dependent(s) (aka "initial applicant w/dependent(s)"), and the child(ren) receives a "pass" in biographic vetting, aka Risk Assessment. Dependents may accompany their parent/guardian to their enrollment interview. Dependents not accompanying their parent/guardian to their interview would be subject to photo collection and document verification upon first travel. Dependents who accompany the parent/guardian to their enrollment interview may be approved after photo collection and document verification if the parent/guardian is approved, and the required photo capture and document verification upon first travel would be overridden.

OR

2. Parent/guardian is an approved member and adds new dependent(s) ("Add Dependent(s)" function). Each dependent added to an account would undergo biographic vetting. If a "pass" in vetting is obtained, the child would be auto approved and be subject to photo collection and document verification upon first travel.

CBP will seek to capture the minors' enrollment photos through Simplified Arrival upon first encounter. CBP also plans to analyze how best to apply this process to existing applicants pending vetting and/or enrollment.

CBP retains discretion to pursue full enrollment and biometric vetting including fingerprint collection for all minors such as in confirmation of facility security check results and NCIC matches.

Once approved, all minors would be subject to recurrent vetting, enhanced vetting and other enforcement actions such as targeted and random inspections to ensure compliance with program eligibility requirements.

By implementing this tri-phase approach, the Global Entry program can remove the fingerprints and interviews from the minor application process while still maintaining strong security measures. Minors will benefit from a more streamlined application process, reducing the burden on both them and their guardians.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information?	☐ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information[2]

[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

Please check all that apply.	☒ 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)[3] ☐ 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.

TTP collects the following data elements as part of the application/TTP process:

- Name
- Date of birth
- Place of birth
- Phone number (now a required field)
- Address history
- E-mail address
- IP Address
- Employment history

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.

[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*

- Travel history
- Citizenship
- Travel document information
- Conveyance (vehicle) information, which must be registered for travel into the United States
- Fingerprints
- Photographs
- CBP generated unique ID

TTP Applicant Information Shared with NTC

1. Name (last, first, mi)
2. Alias names (last, first, mi)
3. Guardian info (for minors)
4. Date of Birth (MM/DD/YYYY format)
5. Place of Birth (City and Country)
6. Country or Countries of Citizenship
7. Travel Document(s) (driver's license, passport/passport card, birth certificate, visa/ESTA, I-94/I-94W, I-551, parole document)
8. Residential address history for past five years
9. Mailing address
10. E-mail address
11. U.S. destination address (for non-US residents)
12. Phone numbers (business/work, cell, home)
13. Vehicle information (plate/make/model/year/VIN/registered owner) if enrolling a vehicle
14. U.S. contact information (for non-US residents)
15. Travel history for past five years
16. Employment for past five years

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.

☐ Social Security number	
☒ Alien Number (A-Number)	
☐ Tax Identification Number	☐ Social Media Handle/ID
☒ Visa Number	☒ Driver's License/State ID Number
☒ Passport Number	☒ Biometric identifiers *(e.g., FIN, EID)*
☐ Bank Account, Credit Card, or other financial account number	

[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.

	☒ Biometrics.[5] *Please list modalities (e.g., fingerprints, DNA, iris scans):* **Fingerprints, photograph** ☐ Other. *Please list: Click here to enter text.*
3(b) Please provide the specific legal basis for the collection of SSN:	N/A
3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.	
N/A	
3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[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: Trusted Traveler number (PASSID), CBSA Client ID for NEXUS and FAST ID for FAST ☐ By a non-unique identifier or other means. Please describe: *Click here to enter text.*

[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 accomplished. IDENT 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.

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]	The disposition of records generated by TTP PTA is covered under DAA-0568-2020-0002 which has been approved by NARA. Cutoff Instructions: Cutoff upon membership expiration or revocation, application denial, account closure, or application cancellation. Retention Period: Destroy 3 year(s) after cutoff.
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)**?**	Automatic purge

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: For the purposes of traveler validation, TTP shares PII with the following CBP applications: Global Entry portals, applications covered within the Traveler Screening Security Authorization Package (Simplified Arrival (SA)), Automated Commercial Environment (ACE), Advanced Passenger Information System (APIS), Electronic System for Travel Authorization (ESTA), Biometrics Services, Consolidated Secondary Inspection System (CSIS), and Reporting Outlying Area Mobile (ROAM). TTP also shares data with CBP's Analysis Targeting System Unified Passenger (ATS-UPAX). ATS will be conducting the vetting for trusted traveler applications.

[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.

	TTP shares data with CBP's Systems, Applications, and Products in Data Processing for the purpose of reconciling TTP payments Outside CBP, TTP shares information with the following DHS Components: TSA – TTP shares with Secure Flight Phase II for TSA's Known Traveler Project. NPPD – TTP shares biographic and biometric information with Homeland Advanced Recognition Technology (HART) used by the Office of Biometric Identity Management (OBIM) as part of the enrollment process. HART performs watch list and criminal history checks through IAFIS as part of this process. NPPD – TTP has a connection available for information sharing with NPPD's CSAT Personnel Surety Application, part of their CFATS program. Enterprise Reporting – Provides report capabilities
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: TTP connects with, and shares PII with: Government Printing Office (GPO) – for the purpose of printing and mailing ABTC and Trusted Traveler membership cards. Canada Border Services Agency (CBSA) – for the purpose of exchanging NEXUS and U.S./Canada FAST enrollment data. Partner Government Agencies – for the purpose of vetting their citizens. Applicant data may also be shared via secure email with border authorities from PGAs that do not have an electronic interface with TTP in order to do vetting

	National Counterterrorism Center (NCTC) for vetting
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: There are MOUs and ISAs with external partners.
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: Through audit logs. ☐ 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 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.[13]

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.*

[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/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.

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. 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:	Click here to enter text.
Date submitted to Component Privacy Office:	**October 20, 2023**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	October 25, 2023

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

(b) (5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6)
DHS Privacy Office Approver (if applicable):	Click here to enter text.
PRIVCATS ID Number:	**0015679**
Date adjudicated by DHS Privacy Office:	October 25, 2023
PTA Expiration Date:	October 25, 2024

DESIGNATION

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

Determination:	☐ Project, Program, System in compliance with full coverage. ☒ Project, Program, System in compliance with interim coverage. ☐ Project, Program, System in compliance until changes implemented. ☐ Project, Program, System not in compliance.
PIA:	**New PIA is required.** DHS/CBP/PIA-002 Global Enrollment System; Trusted Traveler Program (TTP) **[forthcoming]**
SORN:	**System covered by existing SORN** DHS/CBP-002 Trusted and Registered Traveler Programs, March 11, 2020, 85 FR 14214

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)