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 serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, technologies, rulemakings, programs, information sharing arrangement, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If a compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office will send you a copy of the relevant compliance template to complete and return.

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)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	Automated Targeting System (ATS) Mobile Referral Application (App)		
DHS Component:	Customs and Border Protection (CBP)	Office or Program	Office of Field Operations
Date of last PTA (if applicable):	**January 13, 2020**		
If pilot, pilot start date:	**N/A**	Pilot end date:	**N/A**

MOBILE APPLICATION DEVELOPMENT PROGRAM/BUSINESS OWNER

Name:	(b)(6) (b)(7)(C)		
Office:	**CBP/OFO**	Title:	CBP Officer/Program Manager
Phone:	(b)(6) (b)(7)(C)	Email:	(b)(6) (b)(7)(C) cbp.dhs.gov

OIT MOBILE APPLICATION DEVELOPMENT LEAD

Name:	(b)(6) (b)(7)(C)		
Office:	TASPD	Title:	IT Specialist
Phone:	(b)(6) (b)(7)(C)	Email:	(b)(6) (b)(7)(C) @cbp.dhs.gov

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

Mobile App Specific-PTA QUESTIONS

1. Purpose of DHS Mobile Application

1) Describe the purpose of the DHS mobile application[1]. *Please provide a general description of the mobile application and its purpose, including how it supports the DHS mission, in a way a non-technical person could understand. If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.*

Overview

U.S. Customs and Border Protection (CBP), Office of Field Operations (OFO), is submitting this updated PTA for the Automated Targeting System (ATS) Mobile Referral, which is a mobile application, accessible to CBP government employees and contractors, and provides real-time secondary referral information on any CBP workstation, tablet, or mobile device. Recently CBP added the CBP Traveler Verification Service (TVS) into the ATS Mobile Referral App. This is a new functionality and was not incorporated into the previously adjudicated ATS Mobile Referral PTA (dated: January 13, 2020). TVS is used to collect biometric photographs from individuals and verify the identity of individuals. ATS Mobile Referral App collects, uses, and maintains personally identifiable information (PII) from members of the public.

The ATS Mobile Referral App is used by CBP to query individuals (members of the public), and conveyance. CBP officers (CBPOs) and CBP Agriculture Specialists (CBPAs) use the ATS Mobile Referral App to: see referral package details prior to engaging travelers; run queries on persons and vehicles (in CSIS/Unified Secondary); add secondary inspection details and comments; closeout negative inspections; and access and use the ATS Super Query function to query multiple data sources for records of interest, etc. CBP Border Patrol Agents have access to Mobile Referral, but by policy do not use the application to document secondary exams. It is only used for situational awareness. The ATS Mobile Referral App can be used in the air, land, or sea environment. When using the mobile app in the air environment the user has the ability to display flight manifests and processing status of all inbound or outbound flights for selected airports of entry. The ATS Mobile Referral App reduces the time CBPOs and CBPAs spend on data entry and provides CBP employees additional time to focus on enforcement activities.

The ATS Mobile Referral App retrieves information by the following personal identifiers: Full Name (Last, First, Middle); Date of Birth; Photos (i.e. e-Passport Photo search, photo of a face of a foreign national traveler); and Document Number (i.e., Passport, Visa, LPR card).

ATS Mobile App Access and Authentication

Applications are available only inside the firewall via the CBP Intranet. CBP employees, depending on the area of operation and once approved for access, can download the appropriate applications. Access is requested via outlook through the ATS Access Requests inbox and must be approved by the employee's immediate supervisor. Access to ATS Mobile Referral is only granted to CBP personnel who have completed a background investigation (BI), and have an active ATS and TECS profile.

[1] DHS defines DHS Mobile Application (DHS Mobile App) as a native software application that is developed by, on behalf of, or in coordination with DHS for use on a mobile device (e.g., phone or table) by DHS employees and/or the public.

The mobile application user is verified in multiple ways: 1) PIV enabled on a desktop pc, laptop, or tablet; 2) User Hash ID and ATS Profile password; and 3) Air watch enabled using derived PIV credentials for any android or IOS smartphone device.

The suite of ATS Mobile apps can be accessed from the following:

- Mobile device (i.e. smartphone, tablet, etc.). The CBP Government employee must agree to a privacy notice before the mobile application is installed and accessible on the user's mobile device. The standard security notice is visible to the user as they sign into the application. It is also accessible from the help section of the mobile application.

- Desktop PC or laptop. The CBP government employee is required to access a web URL link. The user must agree to a privacy statement before the web link URL is accessible on the user's desktop or laptop computer.

Inspection Process, and Negative Close-Out Functionality

During primary inspection, if an CBPO or CBPA determines that a traveler or conveyance requires further inspection, or finds derogatory information on a subject through any processing system, the subject will be referred to secondary inspection. A referral to secondary inspection will first be generated in the Consolidated Secondary Inspection System (CSIS), a TECS subsystem (CSIS was recently updated with a new user interface and is now called "Unified Secondary" or USEC). CSIS draws information from TECS and captures narrative and other information entered by the CBPO or CBPA over the course of processing a secondary inspection.

The ATS Mobile Referral App acts as a visual representation of secondary inspection referrals in a CBPO's, or CBPA's area of responsibility and links directly to CSIS/USEC to perform queries on individuals and conveyances. CSIS transmits referral biographics, photos, and exam details data to the ATS Mobile Referral App, and the CBPO or CBPA can then use the ATS Mobile Referral App to complete any remaining mandatory fields for the secondary inspection process. Note: The fields will vary based on the type of secondary exam (e.g., admissibility, agriculture or baggage) being performed by the CBPO or CBPA.

Once an individual is signed into the ATS Mobile Referral App, they will be prompted to select one of the following environments: Air, Border Patrol, Land, and Sea. In each environment select, users can view different CSIS referrals, filter through each referral by time, and see the status of each referral (e.g., In work, positive, negative, closed). The upper right hand of the app it displays the location the user is defaulted to. The user can click on the location to either display a different location, select multiple locations to display, or type into the search bar to find a location. The user can view any available CBP site code in the application.

If the user wishes to switch environments, they can select the logout screen and then they will be prompted to select a new environment (e.g., air, border patrol, land, sea). Filters are available for the land mode (e.g., vehicle, pedestrian) and direction (e.g., inbound, and outbound) and the user can select one or all as needed in order to search for a secondary referral.

In addition, the ATS Mobile Referral App provides a mobile option for the CBPO or CBPA to negatively close out three types of secondary exams: admissibility, agriculture, and baggage (vehicle

exams are also cataloged under the "baggage" option). In order to negatively close out the exam, the CBPO or CBPA must access the "Active Referrals" group located in the ATS Mobile Referral App. All negative exams will appear in this group and the officer must choose the correct record to perform the negative closeout of the exam. Once a secondary referral is selected the user will be provided the history of that referral (e.g., VPC images; Package ID #; Referral Type; Direction; Vehicle License Plate #; Vehicle State; Secondary Referral Site; Secondary Referral Via; Secondary Referral Reason; CBPO/CBPA first and last name; date and time of inspection; and the primary officer remarks. The referral will also include the Individual's first, last and middle name; date of birth, country of Residence; Passport #; and gender).

Users can then choose to either exit the referral or close out the negative inspection for either a single inspection, dual inspection, or complex exam (all 3 referral types). Note: The ability to close out all three exams at once is available via the COMPLEX exam option. If the user selected the negative closeout button, the exam automatically closes out in CSIS. If one or all of the three types of secondary exams: admissibility, agriculture, and baggage exams are positive, the officer can no longer use the ATS Mobile Referral App and must use a workstation to complete the exams in CSIS. Information collected in the negative closeout will be automatically sent to CSIS (TECS).

At air locations users can access the flights tab which provides information for all flights arriving in the users AOR. This would be displayed as either an individual flight or aggregate table of all flights. If you select on an individual flight it will display the following information: Flight #; Airline; Departure Date; Departure Location; Arrival Date: Arrival Location; and Flight Status. Users also have the option to export the aggregate data to an excel spreadsheet.

At all sites, there will be a TECS Health tab, which all users can access. This tab will take the user to the TECS System Health Dashboard, which provides a consolidated and summarized view of key performance metrics for the following CBP/OIT/PSPD systems: Automated Passport Control (APC), Border Patrol Client (BPC), Consolidated Secondary Inspection System (CSIS), Global Entry, Pedestrian, Traveler Primary Arrival Client (TPAC), US Arrival, and Vehicle Primary Client (VPC). The TECS Systems Health Dashboard periodically (every 30 seconds) pulls the status from the source monitoring system to display a high-level look at the health of the systems. The TECS System Health Dashboard PTA was recently adjudicated by DHS Privacy on 01/11/2021.

Information Collected

The ATS Mobile Referral App collects information from covered individuals, such as U.S. Citizens and foreign nationals traveling int and out of the United States. The following information is collected from individuals (members of the public) and/or CBP Employees:

<u>Secondary Inspection Detail:</u>

- Disposition (class of admission or a description of the action taken on an individual, based on a CSIS code)
- CBP employee performing inspection (first and last name)
- Start Time/End Time of Inspection

<u>Inspection results, "negative closeout" button:</u>

- Type of Secondary Exam: baggage, agriculture, admissibility, or Complex. (Note: Complex refers to all 3 exams at once. Also, vehicle exams are cataloged as baggage here.)
- Vehicle search performed, if applicable

- Equipment used
- Number of bags examined
- Race
- Hispanic: yes or no. (Mandatory Field in CSIS)
- Comments

New Collection:
- Facial Photo – Used to conduct facial verification comparison through the CBP TVS.

New Use Case: CBP Traveler Verification Service (TVS)
CBP recently incorporated a new feature, Traveler Verification Service (TVS), into the ATS Mobile Referral App, which allows CBPOs to use a mobile device or desktop computer camera to capture a facial photo of a traveler. Identity verification is often a reason for referral. Verification of a document or citizenship can be verified with facial verification. CBP uses the identity verification feature to confirm that the individual matches the travel document he or she is presenting for inspection. CBP uses the TVS technology to match photographs already accessible from existing ATS holdings and ATS interfaces and mirror the existing biographic vetting process. A super query of the traveler biographics provides photographs already accessible from existing holdings are photographs captured by CBP during previous entry inspections, photographs from U.S. passports and U.S. visas, immigration records, and photographs from prior DHS apprehensions and encounters. TVS will conduct a live photo, 1:1, against the photos retrieved from the supe query. The photos will be captured in the ATS Mobile Referral Application but will not be stored on the mobile application.

Retention
ATS Mobile Referral Application does not hold any records. Depending on the data type, the system of record is either ATS, CSIS/Unified Secondary, or TECS. Transactional data goes into CSIS/Unified Secondary and inspectional results go to TECS. Any non-transactional and non-inspectional data processed by ATS Mobile is maintained by the ATS back-end system.

Applicable Federal Regulations:

36 CFR 1230.10(a): "Records must not be destroyed except under the provisions of NARA-approved agency records schedules or the General Records Schedules issued by NARA"
36 CFR 1230.3: "Unlawful or accidental destruction (also called unauthorized destruction) means disposal of an unscheduled or permanent record; disposal prior to the end of the NARA-approved retention period of a temporary record (other than court-ordered disposal under § 1226.14(d) of this subchapter)

2. Subjects and Users[2] of the Mobile Application?	
a. Who will SUBMIT information into this mobile application? *Please describe below.*	☐ Members of the public. ☒ DHS Employees ☐ DHS Contractors ☐ Other federal employees or contractors.

[2] User means a DHS person using a DHS Mobile App.

Subjects: Covered individuals, such as U.S. Citizens and foreign nationals traveling in and out of the U.S. **Users:** CBP Employees, including CBP Officers (CBPOs), and CBP Agents (CBPAs) will submit information from and about members of the public.	
b. Who will USE the information submitted to CBP from this mobile application? *Please describe below.*	☐ Members of the public. ☒ DHS Employees ☐ DHS Contractors ☐ Other federal employees or contractors.
CBP employees (CBP Officers and CBP Agents) will use the information to inform vetting and law enforcement-related decisions during secondary processing at ports of entry (POE).	

3) Data to be received by CBP

a) What information will CBP collect through the mobile application[3]? ***List all data elements.***

The ATS Mobile Referral App collects information from covered individuals, such as U.S. Citizens and foreign nationals traveling int and out of the United States. The following information is collected from individuals (members of the public) and/or CBP Employees:

Secondary Inspection Detail:

- Disposition (class of admission or a description of the action taken on an individual, based on a CSIS code)• CBP employee performing inspection (first and last name)
- Start Time/End Time of Inspection

Inspection results, "negative closeout" button:

- Type of Secondary Exam: baggage, agriculture, admissibility, or Complex. (Note: Complex refers to all 3 exams at once. Also, vehicle exams are cataloged as baggage here.)
- Vehicle search performed
- Equipment used
- Number of bags examined
- Race
- Hispanic: yes or no. (Mandatory Field in CSIS)
- Comments

New Collection:

- Facial Photo – Used to conduct facial verification comparison through the CBP TVS.

[3] If a DHS Mobile App is collecting PII from users, then a Privacy Statement is provided at the point of collection. This Privacy Statement may be provided through a pop-up notification on the DHS Mobile App screens where PII is collected or via another mechanism approved by the Chief Privacy Officer.

b) How is the information stored? *Please describe below.*	☐ Locally on the mobile device. X In a backend CBP IT system. ☐ With a third party vendor. ☐ Other. Describe_____
ATS Mobile Referral Application does not hold any records. Depending on the data type, the system of record is either ATS, CSIS/Unified Secondary, or TECS. Transactional data goes into CSIS/Unified Secondary and inspectional results go to TECS. Any non-transactional and non-inspectional data processed by ATS Mobile is maintained by the ATS back-end system. Applicable Federal Regulations: 36 CFR 1230.10(a): "Records must not be destroyed except under the provisions of NARA-approved agency records schedules or the General Records Schedules issued by NARA" 36 CFR 1230.3: "Unlawful or accidental destruction (also called unauthorized destruction) means disposal of an unscheduled or permanent record; disposal prior to the end of the NARA-approved retention period of a temporary record (other than court-ordered disposal under § 1226.14(d) of this subchapter)	
c) Does the mobile application collect Social Security number (SSN) or other elements of Sensitive Personally Identifiable Information (SPII)[4]? Check all that apply.	☐ Social Security number ☐ Alien Number (A-Number) ☐ Passport Number ☐ Bank Account, Credit Card, or other financial account number X Other. Describe_____ • **Any supporting identity and immigrant eligibility documents.** • **Biometric Facial Image**
d) List the *specific authority* to collect SSN or these other sensitive PII elements	
Authorities supporting CBP's collection and use of the ATS Mobile Referral Application data include: -1996 Illegal Immigration Reform and Immigrant Responsibility Act - Immigrations and Nationality Act (INA) - Title 8 U.S.C: Policy Memo (Nationwide Deployment of the Consolidated Secondary Inspection System, Sept 10, 2010)	
e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.	

[4] DHS defines Sensitive Personally Identifiable Information (SPII) meaning PII which, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some types of PII, such as Social Security Number (SSNs), Alien Registration Number, and biometric identifiers, are always sensitive. Other types of PII, such as an individual's driver's license number, financial account number, citizenship or immigration status, or medical information are SPII if DHS maintains them in conjunction with other identifying information about the individual. In some instances the context surrounding the PII may determine whether it is sensitive. For example, a list of employee names by itself may not be SPII, but could be if it is a list of employees who received poor performance ratings.

Travelers without a travel document or possible fraudulent document may be required to provide additional documentation. Fingerprints are not collected in the ATS Mobile Referral App. Fingerprint capture is collected in CSIS and/or Mobile Query and results captured in the comments are in Referral.	
f) Does the mobile application collect other types of sensitive information[5]? Check all that apply.	☐ Location Information[6] X Photos/Videos ☐ Mobile Device ID ☐ Metadata[7] ☐ Other. Describe_____
g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.	
Photos are captured through the ATS Mobile Referral App so that officers can determining identity and/or citizenship of a traveler, in a standard measurable format rather than relying on a visual comparison, during secondary enforcement exams.	

4. Notices

a) Are individuals provided notice[8] at the time of collection by DHS? If yes, please include a copy of the notice(s) with this PTA upon submission.	X Yes. Please describe. ☐ No. Please describe.
Yes, the Privacy Notice is embedded into the mobile referral application. The privacy notice is only for the CBP employees using the mobile application. **U.S. Customs and Border Protection** **U.S. Department of Homeland Security** **For Official Use Only // Law Enforcement Sensitive** You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following:	

[5] Sensitive content means information that may not be PII, but raises privacy concerns because it may be related to the use of PII (e.g., location information, mobile device ID, or metadata).

[6] Location Information means the ability of a mobile device to know a user's current location and/or location history as determined by Global Positioning System (GPS) and/or other methods.

[7] Metadata means the information stored as the description of a unique piece of data and all the properties associated with it. For example, mobile device metadata may include the time and duration of all phone calls made from a particular mobile device, the mobile device IDs of the mobile devices involved in the phone calls, and the locations of each participant when the phone calls occurred.

[8] Provided upon each update to the mobile app to specifically identify any changes to the uses of information from previous versions of the app.

▪ You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting, stored on, originated from or directed to this information system. At any time, and for any lawful government purpose, the government may monitor, intercept, search and seize any communication or data transiting, stored on, originated from or directed to or from this information system.

▪ The government may disclose or use any communications or data transiting, stored on, originated from or directed to or from this information system for any lawful government purpose.

▪ You are NOT authorized to process classified information on this information system.

For Official Use Only: Do not disclose data in screenshot format, create hard or electronic copies, or cut and paste into TECS. Please ensure that dissemination of this information is limited and controlled in a manner consistent with DHS and CBP policies. Privacy Act: An improper disclosure of personal information contained in this system would constitute a violation of the Privacy Act (5 U.S.C. 552a). Violators could be subject to a fine of not more than $5,000 per record and removal from employment. Information contained in this system is subject to the 3rd party rule and may not be disclosed to other government agencies without the express permission of the agency supplying the original information.

Trade Secrets Act: This system may contain trade secrets and commercial and financial information relating to the confidential business of private parties. The Trade Secrets Act (18 U.S.C. 1905) provides penalties for disclosure of such information. Customs employees who violate this act and make wrongful disclosures of confidential commercial information may be subject to a personal fine of up to $250,000, imprisonment for not more than one year, or both, and shall be removed from employment.

5. Disclosures	
a) Does the mobile application provide "just-in-time"[9] disclosures to obtain user's affirmative express consent before a DHS mobile app accesses sensitive content or other tools and applications on the mobile device for the first time (e.g., Location services)?	☐ Yes. Please describe. X No. Please describe.
Photo comparison is being conducted during an enforcement exam. Officers can provide an explanation of the process, but no opt-option is built in.	

[9] DHS mobile apps are to be developed so as to obtain users' affirmative express consent before a DHS mobile app accesses sensitive content or other tools and applications on the mobile device for the first time (e.g., location services)

b) Does the mobile application provide any information to third parties (any organization outside of CBP)?	☐ Yes. Please describe. X No. Please describe.
N/A	

6. Opt-out Features	
a) Does the mobile application provide users with independent opt-out features[10] so that users may customize the mobile app's features (e.g., opting out of location based services, while still choosing to utilize other app services) where appropriate?	☐ Yes. Please describe. X No. Please describe.
This app must be used by CBPOs, CBPAs, and U.S. BPAs for specified immigration enforcement activities. They cannot opt-out of these job-related responsibilities or customize the mobile app features. CBP users must physically launch the camera option and press take photo. The traveler does not need to provide consent, since this will only be conducted if identity is in question, during an enforcement exam.	

7. Mobile App-Specific Privacy Policy	
a) Does the mobile application have an App-Specific Privacy Policy[11] that is available to users through the commercial app store as well as within the app? If yes, please include a copy of the App-Specific Privacy Policy with this PTA[12] upon submission.	☐ Yes. Please describe. X No. Please describe.
The public is not accessing the mobile application and the privacy policy is not required for this ATS Mobile Referral App.	

[10] DHS Mobile apps are to provide users with independent opt-out features so that users may customize the mobile app's features (e.g., opting out of location based services, while still choosing to utilize other app services), where appropriate

[11] Engage with DHS Carwash to ensure app security and privacy. If users submit sensitive information through a DHS mobile app, that information is encrypted in transit and immediately transferred to a protected internal DHS system that is compliant with existing DHS IT security policy. Sensitive content that a DHS mobile app accesses or uses for the benefit of the user, but that DHS does not need to collect (e.g., location information), should be locally stored within the mobile app or mobile device. This info should not be transmitted or shared with DHS

[12] Privacy Threshold Analysis (PTA) means both the DHS Privacy Office process to be followed and the document used to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the proposed use, identifies the legal authorities for the proposed use, and describes what PII, if any, is collected (and from whom) and how that information is used. PTAs are adjudicated by the Chief Privacy Officer

8. DHS Carwash process?	
a) Has this mobile application been through the DHS Carwash[13] process?	X Yes. **Please provide the results of the Carwash with this PTA.** ☐ No. Please describe.
The DHS AppVet results for Android and iOS are attached to this PTA submission.	

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:	**June 15, 2021**
Date submitted to DHS Privacy Office:	June 15, 2021
Component Privacy Office Recommendation: *Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.*	
(b)(5)	

[13] DHS Carwash is the service sponsored by DHS Office of the Chief Information Officer (OCIO) that provides development teams with a continuous integration, build, test, source code management, and issue tracking environment for building DHS Mobile Apps. The shared platform provides application lifecycle management and support for mobile apps built on development frameworks. The DHS Carwash also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility.

(b)(5)

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
PCTS Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	June 16, 2021
PTA Expiration Date	June 16, 2022

DESIGNATION

Privacy Sensitive Application?	**Yes If "no" PTA adjudication is complete.**
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Specialized training required. ☒ Other. **A Mobile App Privacy Policy is Required**
PIA:	**New PIA is required.** If covered by existing PIA, please list: DHS/CBP/PIA-006 Automated Targeting System; DHS/CBP/PIA-021 TECS System: Platform; DHS/CBP/PIA-056 Traveler Verification Service; Forthcoming Mobile Inspection Processing PIA If a PIA update is required, please list: Click here to enter text.
SORN:	**System covered by existing SORN** If covered by existing SORN, please list: DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297; DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778 If a SORN update is required, please list: Click here to enter text.
DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*	

(b)(5)

(b)(5)