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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One™ Mobile Application – Advance Information for Certain Undocumented Individuals, including Individuals with Advance Authorization to Travel to the United States to Seek Advance Parole
DHS Component:	U.S. Customs and Border Protection (CBP) Office of Field Operations (OFO) & Office of Information and Technology (OIT)
Date of last PTA:	N/A
If pilot, pilot start date:	N/A

MOBILE APPLICATION DEVELOPMENT PROGRAM/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	CBP/OFO/PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

Mobile App Specific-PTA QUESTIONS

1. Purpose of DHS Mobile Application

1) Describe the purpose of the DHS mobile application. *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.*

In response to the challenges presented by the high number of migrant encounters along the U.S. Southwest Border, the U.S. Customs and Border Protection (CBP) is creating a new Advance Travel Authorization" (ATA) capability in CBP One™. CBP is limiting eligibility to use this capability to citizens of countries that meet the criteria created by DHS. This includes countries suffering under repressive authoritarian regimes as well as experiencing significant economic and humanitarian crises. Appendix A of this PTA includes the names of eligible countries. Use of CBP One is voluntary.

In partnership with United States Citizenship and Immigration Service (USCIS) and the I-134[1] sponsorship process, CBP is developing a new "Request Advance Travel Authorization" capability in CBP One that will include the collection of a biometric and biographic information which allows travelers to gain advance authorization to travel via air to the United States to seek parole. Travel authorization with sponsorship enables populations to approach the U.S. via expanded modes of transportation and/or to approach the border at defined entry schedules drastically aiding in CBP's ability to monitor populations and control encounters across U.S. borders.

To accomplish the above, Individuals will use the CBP One™ Mobile Application to capture their biographic and biometric information and transmit the data CBP (b)(7)(E) (b)(7)(E)

Once the individual is logged in to CBP One™, they are must to select "Traveler", then "Air", then "Request Air Travel Authorization". First time users will be prompted to select their preferred language (English or Spanish). After these steps are complete, the user must provide their First and Last name as part of a "Profile" then provide the Alien Registration Number (A-number) created by USCIS and provided to the user once their I-314 is approved as well as their date of birth (DOB) and passport number as it is listed in their myUSCIS[2] account. The

[1] Additional Information on the 10134 Process is *available at* https://www.uscis.gov/i-134

[2] For more information on myUSCIS please see the link *available at* https://my.uscis.gov

myUSCIS account is where the initial request for advance parole, sponsor application and ultimate results of the request for authorization to travel via air will be managed and viewable by the user.

Initially, the traveler may enter this data manually and use the camera on their phone to capture a photograph. However CBP will transition to utilizing an embedded technology to capture the Machine Readable Zone (MRZ) and eChip for citizens of countries who offer e-Passports. Once CBP transitions to utilizing the MRZ scanner, the user is prompted to scan the passport Machine Readable Zone. Once the scan is successful, CBP One will use Near Field Communication (NFC) capability to retrieve additional information stored within the e-chip (all the biographic information displayed on passport page, (photograph and country signing certificate to certify the authenticity of the passport). The CBP One™ application will retrieve the photo from the eChip and instruct the user to take a live photo of his or herself or of the intending traveler (incases when a third party such as a family member is completing the authorization on behalf of the traveler). The app validates the "liveness" of the photo, in other words, it confirms that a "live" face was captured. Once this process is complete, the user is presented with a confirmation screen informing them of the successful submission and directing them to their myUSCIS account for updates on the status of their request. For individuals arriving with approved immediate family members, the process discussed above will need to be repeated, and CBP One™ will create a single submission for all immediate family members.

If the user experiences issues and the application is unable to access the e-Passport or recognize the biographic information, they can choose to reenter the information. If the second attempt is unsuccessful, the user will be advised their request cannot be validated and to refer to their myUSCIS account to ensure their I-134 has been approved.

All information will be stored in the ATIS system and (UPAX) within ATS.

The biographic and passport number as well as the e-Passport and live photo will be transmitted to ATIS for validation and storage. CBP One™ will immediately discard both photos. Once the data is validated in ATIS against the information submitted from USCIS, it will be submitted to the Unified Passenger (UPAX) within the Automated Targeting System (ATS) system[3] checks to identify individuals who may pose a risk to national security, border security or public safety. These checks are similar to the checks conducted by CBP during the

[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006(e) (2022), *available at* https://www.dhs.gov/privacy-impact-assessments. CBP is currently developing an update to this PIA to discuss the CBP Advanced Travel Authorization (ATA) program and ATS vetting procedures.

primary or, in some cases, secondary inspection process. The vetting results will be returned to ATIS along with a recommendation whether to grant the requester and co-travelers (immediate family only) the authority to travel. This recommendation will be transmitted to USCIS to be displayed in the users associated myUSCIS account. [4]

While no information is stored locally in the CBP One™ application or on a user's device, the data submitted through CBP OneTM application will be stored in the Amazon Web Services cloud for 365 days for purposes of reporting aggregate data for CBP leadership.

2. Subjects and Users 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.

Certain undocumented noncitizens, or immediate family members, from eligible countries with approved I-134s to seek the Advance Authorization to Travel to the United States to Seek Parole may submit information into this mobile application.

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 Officers will conduct pre-arrival vetting information to inform a recommendation for USCIS to grant the authority to travel for purposes of applying for parole.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES (USCIS), PRIVACY IMPACT ASSESSMENT FOR MYUSCIS: DHS/CBP/PIA-064 (2019), *available at* https://www.dhs.gov/privacy-impact-assessments.

3) Data to be received by CBP

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

CBP One™ collects the same information that CBP would otherwise collect during the primary and/or secondary inspection, including:

- Facial photograph
- Photo from passport eChip
- First and last name
- Date of birth
- Passport Number

For individuals arriving with immediate family members, the process discussed above will need to be repeated, and CBP One™ will create a single submission for all family members.

b) How is the information stored? *Please describe below.*	☐ Locally on the mobile device. ☒ In a backend CBP IT system. ☐ With a third-party vendor. ☐ Other. Describe________

All information will be stored in the ATIS system and (UPAX) within ATS.

The biographic and passport number as well as the e-Passport and live photo will be transmitted to ATIS for validation and storage. CBP One™ will immediately discard both photos. Once the data is validated in ATIS against the information submitted from USCIS, it will be submitted to the Unified Passenger (UPAX) within the Automated Targeting System (ATS) system checks to identify individuals who may pose a risk to national security, border security or public safety. These checks are similar to the checks conducted by CBP during the primary or, in some cases, secondary inspection process. The vetting results will be returned to ATIS along with a recommendation whether to grant the requester and co-travelers (immediate family only) the authority to travel. This recommendation will be transmitted to USCIS to be displayed in the users associated myUSCIS account.

While no information is stored locally in the CBP One™ application or on a user's device, the data submitted through CBP One™ application will be stored in the Amazon Web Services cloud for 365 days for purposes of reporting aggregate data for CBP leadership.

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	□ Social Security number
other elements of Sensitive Personally Identifiable Information (SPII)? Check all that apply.	X **Alien Number (A-#)** X **Passport Number** □ Bank Account, Credit Card, or other financial account number (via pay.gov) □ Other. Describe: Biographic and biometric data (see 3a)

d) List the *specific authority* to collect SSN or these other sensitive PII elements

The following CBP legal authorities permit the collection of border crossing information:

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638; Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354; Aviation and Transportation Security Act of 2001 (ATSA); Enhanced Border Security and Visa Reform Act of 2002.

e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

This information collection is required to streamline processing at the airport.

f) Does the mobile application collect other types of sensitive information? Check all that apply.	☐ Location Information[7] ☒ **Photos/Videos** ☒ **Mobile Device ID** ☒ **Metadata** ☐ Other. Describe________ Device ID/Metadata - This information is collected by CBP One™ as a whole. This action is performed at log in. This is used for other capabilities for push notification. We do not use this data for this use case, but there is no way to turn on and off based on capability.

g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.

The collection of the eChip photo and live photo is to verify the person submitting the information through the mobile application is the same as the person who the passport was issued and therefore CBP has confidence in associating the biographic, document and photo information and as well as the resultant risk assessment.

4. Notices

a) Are individuals provided notice[9] at the time of collection by DHS? If yes, please include a copy of the notice(s) with this PTA upon submission.	☒ Yes. Please describe. ☐ No. Please describe.

CBP One™ App Specific: Notice of the collection of PII will be provided to the user in the Terms and Conditions before entering the application. A copy of this document is provided with the submission of the PTA.

Functionality Specific: Additionally, the individuals collecting information on behalf of undocumented individuals and submitting this information to CBP, through CBP One™, are responsible for notifying the individual.

5. Disclosures

a) Does the mobile application provide "just-in- time"[10] 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. ☒ No. Please describe.

N/A, all information is submitted via the undocumented individual, or by another individual on behalf of the undocumented individual. The undocumented individual voluntarily submits their information to CBP.

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

N/A

6. Opt-out Features

a) Does the mobile application provide users with independent opt-out features[11] 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. ☒ No. Please describe.

Use of the CBP One™ mobile application is voluntary. The mobile device camera must be enabled by the user prior to launching this functionality. If the user opts-out to enabling their device camera, they will be unable to continue through this functionality and sent back to the home screen of the app.

7. Mobile App-Specific Privacy Policy

a) Does the mobile application have an App-Specific Privacy Policy 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 upon submission.	☒Yes. Please describe. No. Please describe.

The Privacy Policy is listed in the application's Terms and Conditions. DHS approved a CBP One™ Mobile App Privacy Policy with the original submission of the CBP One™ PTA.

8. DHS Carwash process?

a) Has this mobile application been through the DHS Carwash[14] process?	]Yes. **Please provide the results of the arwash with this PTA.** No. Please describe.
CBP has conducted multiple AppVet scans on CBP One. CBP will conduct a new DHS AppVet after the May 23, 2022 deployment for this capability. CBP does no expect the results to be different from previous scans.	

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:	**September 26, 2022**
Date submitted to DHS Privacy Office:	September 26, 2022

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)

(b)(5)

PRIVACY THRESHOLD ADJUDICATION
(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
PCTS Workflow Number:	0023211
Date approved by DHS Privacy Office:	September 28, 2022
PTA Expiration Date	September 28, 2023

DESIGNATION

Privacy Sensitive Application?	**Yes**

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. **X** Privacy Act Statement required. **X** Privacy Impact Assessment (PIA) required. **X** System of Records Notice (SORN) required. □ Specialized training required. Other.
PIA:	**New PIA is required.** If a PIA update is required, please list: DHS/CBP/PIA-068 CBP One™ Mobile Application **(appendix update required)**; DHS/CBP/PIA-021 TECS System: Platform; DHS/CBP/PIA-006 (e) Automated Targeting System (ATS) **(appendix update required)**; **forthcoming Collection of Advance Information from Certain Undocumented Individuals at the Land Border**
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

DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*

(b)(5)

(b)(5)

(b)(5)

Homeland
Security

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One™ Mobile Application, New PTA- International Organization (IO)/Non-Governmental Organizations (NGOs) Use Case for Processing Undocumented Noncitizens (Afghan Refugees)		
DHS Component:	Customs and Border Protection (CBP)	Office or Program	OFO/PPAE
Date of last PTA (if applicable):	N/A		N/A
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/PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

OIT MOBILE APPLICATION DEVELOPMENT LEAD

Name:	(b)(6), (b)(7)(C)		
Office:	CBP/OIT	Title:	Supervisory IT Specialist
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

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.*

DHS is working with International Organizations (IOs) and Non-Governmental Organizations (NGOs), identified by the United States (U.S.) Department of State (DoS), to screen and verify the identity of undocumented noncitizens (Afghan Refugees) awaiting resettlement into the United States. Depending on the circumstances of their arrival into the United States, some undocumented noncitizens lack a valid travel document and therefore may be unable to travel domestically. CBP has updated CBP One™ to allow IOs/NGOs, on behalf of an undocumented noncitizen, to submit information to CBP to verify the identity of undocumented noncitizen during the resettlement process.

CBP is submitting this new PTA to document a new population of individuals collected through the International Organization (IO) persona in the CBP One™ mobile application (app). The IO persona will be used by IOs/NGOs to collect information from undocumented noncitizens (Afghan Refugees) and verify their identity prior to traveling domestically within the United States.

Access

CBP will authenticate and permit IOs/NGOs access to the CBP One™ mobile app, IO persona. Users working for an IO/NGO will download and access CBP One™ in the same manner as all other users of CBP One™. CBP will determine whether a user can have access to IO persona based on the information the user inputs to create a Login.gov account. Eligible IOs/NGOs will provide email domain names to CBP and CBP will open access to the functionality within CBP One™ to users who created Login.gov accounts using that email domain.

Process

Once a user has access to the IO persona in CBP One™, they will be able to use the application to facilitate processing of undocumented noncitizens awaiting resettlement in the United States. To do this, an IO user, with the consent of and on behalf of the individual, will take a photograph of the undocumented noncitizen and, using the Traveler Verification Service (TVS) facial comparison technology, match the individual seeking resettlement with a photograph in an existing staged gallery. The staged gallery is populated with images from the SaAW database/ATS. ATS retrieves refugees' facial photographs from IDENT, and these facial photographs are sent to the staged refugee gallery in the SaAW database. In addition, the SaAW database pulls I-94 biographic information from the I-94 database and transmit this information back to the CBP One™ mobile application.

[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.

If a match is made, CBP One™ will return a green check mark with the First Name, Last Name, Date of Birth, Alien Identification Number (A-number) (if available), citizenship of the traveler, and a facial photograph of the traveler (if available). CBP One™ uses the biographic and information pulled from SaAW, to match against the information in the I-94 database. The facial photograph of the traveler, returned through CBP One™, is pulled from IDENT. The IO can then check the biographic information and biometric information in CBP One™ against the undocumented noncitizens alternate form of identification (i.e., a printed I-94 or other form of identification issued by the resettlement centers).

CBP One will return a red "X" if no match is found. If the undocumented noncitizen is not found in the CBP One™ application, they must use other means of verifying identity such as a printed I-94 or other form of identification issued at safe haven or resettlement areas. IO/NGO users will not have the option to search by the undocumented noncitizens biographic or Alien number through the CBP One™ application.

Retention

As with other CBP One™ uses, no information is stored locally on the device. IOs/NGOs and CBP will not store the facial photograph.

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.

International Organizations (IOs)/Non-Government Organizations (NGOs) provisioned users, submit information from undocumented noncitizens (Afghan Refugees) into the CBP One™ mobile application, IO persona.

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.

IOs/NGOs will use the information submitted through CBP One™ to verify identity of undocumented noncitizens.

3) Data to be received by CBP

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

a) What information will CBP collect through the mobile application[3]? ***List all data elements.***	
Live Facial Photograph	
b) How is the information stored? *Please describe below.*	☐ Locally on the mobile device. ☐ In a backend CBP IT system. ☐ With a third party vendor. ☒ Other. Describe________
As with other CBP One™ uses, no information is stored locally on the device. IOs/NGOs and CBP will not store the facial photograph collected through the CBP One mobile app.	
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 ☐ Other. Describe________
d) List the *specific authority* to collect SSN or these other sensitive PII elements	
N/A	
e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.	
N/A	
f) Does the mobile application collect other types of sensitive information[5]? Check all that apply.	☐ Location Information[6] ☒ Photos/Videos **(Live facial photograph)** ☐ Mobile Device ID ☐ Metadata[7] ☐ Other. Describe________

[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.

[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.

[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.

g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.
Undocumented noncitizens (Afghan Refugees) may not have a valid travel document to present to an IO/NGO for identity verification. The CBP One™ Mobile App collects the facial photograph from undocumented noncitizens in order to verify their identity prior to traveling domestically throughout the United States.

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.	☒ Yes. Please describe. ☐ No. Please describe.
CBP One™ App Specific: Notice of the collection of PII will be provided to the user in the Terms and Conditions before entering the application. IO persona Specific: Additionally, the IO/NGO collects information from undocumented noncitizens (Afghan Refugees) and submits that information to CBP, through CBP One™. The IO/NGO is responsible for notifying each traveler about information collected and submitted to CBP through the CBP One™ mobile app.	

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. ☒ No. Please describe.
N/A	
b) Does the mobile application provide any information to third parties (any organization outside of CBP)?	☒ Yes. Please describe. ☐ No. Please describe.
IOs/NGOs submit and receive information from the CBP One™ Mobile App.	

6. Opt-out Features

[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.

[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)

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. ☐ No. Please describe.

The CBP One mobile app, International Organization (IO) persona, collects the undocumented noncitizens facial photograph in order to verify the identity of the undocumented noncitizen. The IO persona does not have the option to search by the undocumented noncitizens biographic or Alien number. However, undocumented noncitizens have the ability to opt out of providing their live facial photograph to an IO/NGO through the CBP One mobile app. If the undocumented non-citizen chooses to not submit their facial photograph through CBP One, the IO/NGO must use other means of verifying the undocumented noncitizen's identity (i.e., such as a printed I-94 or other form of identification issued at safe haven or resettlement areas).

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. ☐ No. Please describe.

The Privacy Policy is listed in the application's Terms and Conditions. DHS approved a CBP One™ Mobile App Privacy Policy with the original submission of the CBP One™ Mobile App PTA.

8. DHS Carwash process?

a) Has this mobile application been through the DHS Carwash[13] process?	☒ Yes. **Please provide the results of the Carwash with this PTA.** ☐ No. Please describe.

[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

[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.

Completed	

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:	**October 6, 2021**
Date submitted to DHS Privacy Office:	October 7, 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)	

(b)(5)

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:	November 4, 2021
PTA Expiration Date	November 4, 2023

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. Click here to enter text.
PIA:	**PIA update is required.** If covered by existing PIA, please list: DHS/CBP/PIA-006 Automated Targeting System If a PIA update is required, please list: DHS/CBP/PIA-068 CBP One™ Mobile Application; DHS/CBP/PIA-056 Traveler Verification Service
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; DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601 If a SORN update is required, please list:

DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*

(b)(5)

(b)(5)

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One™ Mobile Application – Advance Information for Certain Undocumented Individuals, including Individuals with Advance Authorization to Travel to the United States to Seek Parole Pursuant to the Uniting for Ukraine (U4U) Process
DHS Component:	U.S. Customs and Border Protection (CBP) Office of Field Operations (OFO) Planning, Program Analysis, and Evaluation (PPA&E)
Date of last PTA:	N/A
If pilot, pilot start date:	N/A

MOBILE APPLICATION DEVELOPMENT PROGRAM/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	CBP/OFO/PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

Mobile App Specific-PTA QUESTIONS

1. Purpose of DHS Mobile Application

1) Describe the purpose of the DHS mobile application. *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.*

CBP Privacy is submitting this new PTA to discuss a new functionality of CBP One™, in which certain undocumented individuals, including individuals with advance authorization to travel to the United States to seek parole pursuant to the Uniting for Ukraine (U4U) process, can voluntarily submit biographic information, as well as a facial photograph, to CBP in advance of their arrival at a land Port of Entry (POE). In addition, CBP will also collect location and liveness data from individuals using the CBP One™ mobile application. On April 25, 2022, the advance information capability was rolled out only to eligible Ukrainian citizens and, as appropriate, members of their immediate family, who have an approved advance authorization to travel to the United States to seek parole pursuant to the Uniting for Ukraine (U4U) process. This functionality is available under the ""Traveler" persona. CBP plans to eventually make the advance information submission functionality available to all individuals, including U.S. citizens, who intend to arrive at a land POE. This expansion of access is estimated to take place on May 23, 2022.

Typically, once an undocumented individual arrives at a land POE for processing, CBP Officers (CBPOs) spend significant time collecting and verifying basic biographic data about the individual during the inspection process. One at a time, the CBPOs interview and collect information from such individuals during secondary inspection. The CBPOs manually enter the information into the Unified Secondary System (USEC). This new functionality will streamline processing upon arrival and reduce the amount of manual data entry into primary and secondary processing systems, CBP One™ data will be displayed on the primary inspection screen and available for importation into secondary processing events.

Once the individual is logged in to CBP One™, they are prompted to select "Traveler", then "Land", then "Submit Advance Information". First time users will be prompted to select their preferred language (English or Spanish). After these steps are complete, the user must then select "Add Individual". CBP One™ then collects the same information that CBP would otherwise collect during the primary and/or secondary inspection, including:

- Facial photograph
- First and last name
- Date of birth
- Nationality
- Country/city of birth
- Country of residence
- Travel document information

- Phone numbers
- U.S. address
- Foreign addresses (optional)
- Employment history (optional)
- Travel history (optional)
- Emergency contact information (optional)
- Family information
- Martial information
- Identity documents
- Gender
- Height
- Weight
- Eye color

For individuals arriving with co-travelers, the process discussed above will need to be repeated, and CBP One™ will create a single submission for all co-travelers. CBP One ™ will also collect latitude and longitude coordinates. These coordinates will be sent to CBP to determine whether the submission is occurring within 30 miles of the U.S.- Mexico border. In addition, CBP One™ collects the preparer (person assisting the individual with their submission)'s first and last name and email address.

DHS is working with the Department of State to provide local messaging in Mexico to the populations who would need to utilize CBP One™ to schedule their advance arrival following a U4U travel authorization approval. The messaging will encourage individuals with an approved advance travel authorization who intend to travel to a U.S.-Mexico land border POE to use CBP One™ to inform CBP of their intended date and time of arrival; however, use of CBP One™ is voluntary.

For all individuals accessing CBP One™ on a mobile device, once the individual has entered all biographic information as well as a facial photograph for themselves and any co-travelers, CBP One™ will display available arrival date/times based on the selected land POE. The individual will be offered the opportunity to schedule their desired arrival land POE location, date of arrival, and time of arrival. All individuals accessing CBP One™ on the web will be able to submit the facial photograph as well as the other information through the web, however they will be instructed to utilize the mobile application to select available arrival date/times. All individuals utilizing CBP One™ to schedule or reschedule a presentation date after their initial submission will be required to submit a live facial photograph to access their original submission. While CBP allows individuals to select a desired POE and date/time of arrival, this request does not guarantee that an individual will be processed on a given date or at a given time.

After the data is submitted, the individual is presented with a confirmation screen which displays a confirmation number along with the selected POE and date/time, if applicable. In addition, a confirmation email will be sent to the email address(es) provided under contact information during the CBP One™ submission, or, in the absence of an email within CBP One™, it will be sent to the registered email of the Login.gov account. Prior to arrival at the POE, CBP may use the information submitted by the individual to conduct system checks to identify individuals who may pose a risk to national security, border security or public safety. These checks are identical to the checks conducted by CBP during the primary or, in some cases, secondary inspection process. CBP will not inform the user of the outcome of these checks, but CBPOs will use the information during primary and secondary inspections.

During primary inspection at the POE, the CBPO will use the Simplified Arrival system to take a new facial photograph. This facial photograph will search against multiple CBP Traveler Verification Service (TVS) galleries including a pre-staged "Submit Advance Information" gallery. The "Submit Advance Information" gallery consists of templates that CBP created from the facial photograph submitted by users during the submission process. If there is a match, the information the user submitted through CBP One™, as well as the results of the system checks, will be displayed to the CBPO. If no match is made, CBPOs will manually enter the individual's confirmation number or biographic data to populate Simplified Arrival for processing in primary.

As with any individual who arrives at the POE without documentation, the CBPO will use Simplified Arrival to create a referral to secondary for further processing, to include the confirmation number received from CBP One™. Once referred to secondary, CBP Officers may import the information captured through the CBP One™ application into a USEC event.

2. Subjects and Users 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.

Certain Undocumented individuals, including Individuals with Advance Authorization to Travel to the United States to Seek Parole Pursuant to the Uniting for Ukraine (U4U) Process, may submit information into this mobile application. Additionally, individuals on behalf of undocumented individuals may submit information into this mobile application.

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 Officers (CBPOs) who conduct primary and secondary inspections at Ports of Entry. Pre-arrival vetting information will be used to streamline and expedite CBPOs' processing of individuals, including identifying those who may pose a security threat.

3) Data to be received by CBP

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

CBP One™ collects the same information that CBP would otherwise collect during the primary and/or secondary inspection, including:

- Facial photograph
- First and last name
- Date of birth
- Nationality
- Country/city of birth
- Country of residence
- Travel document information
- Phone numbers
- U.S. address
- Foreign addresses (optional)
- Employment history (optional)
- Travel history (optional)
- Emergency contact information (optional)
- Family information
- Martial information
- Identity documents
- Gender
- Height
- Weight
- Eye color

For individuals arriving with co-travelers, the process discussed above will need to be repeated, and CBP One™ will create a single submission for all co-travelers. CBP One ™ will also collect latitude and longitude coordinates. These coordinates will be sent to CBP to determine whether the submission is occurring within 30 miles of the U.S.- Mexico border. In addition, CBP One™ collects the preparer (person assisting the individual with their submission)'s first and last name and email address.

b) How is the information stored? *Please describe below.*	☒ Locally on the mobile device. ☒ In a backend CBP IT system. ☐ With a third-party vendor. ☐ Other. Describe________

No PII information is stored locally on the individual's device. Individuals submitting directly will have their confirmation number and scheduled POE, day and time saved to their device.

All information will be stored in a segregated database within the backend Unified Secondary system and will be used to run system checks in advance of the expected arrival at the Port of Entry, as well as to pre-populate the Unified Secondary event upon arrival at the POE in order to expedite the Secondary processing.

Unified Secondary is the system of record for all of the data that is being collected by the CBP One Application.

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	☐ Social Security number
other elements of Sensitive Personally Identifiable Information (SPII)? Check all that apply.	☐ Alien Number (A-Number) X Passport Number ☐ Bank Account, Credit Card, or other financial account number (via pay.gov) ☐ Other. Describe: Biographic data (see 3a)

d) List the *specific authority* to collect SSN or these other sensitive PII elements

The following CBP legal authorities permit the collection of border crossing information:

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638; Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354; Aviation and Transportation Security Act of 2001 (ATSA); Enhanced Border Security and Visa Reform Act of 2002.

e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

This information collection is required to streamline processing at the Port of Entry.

f) Does the mobile application collect other types of sensitive information? Check all that apply.	☐ Location Information[7] ☒ Photos/Videos ☒ Mobile Device ID ☒ Metadata ☐ Other. Describe________ Device ID/Metadata - This information is collected by CBP One™ as a whole. This action is performed at log in. This is used for other capabilities for push notification. We do not use this data for this use case, but there is no way to turn on and off based on capability.

g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.

Liveness Photos are collected to verify identification once an individual arrives at a POE.

4. Notices

a) Are individuals provided notice[9] at the time of collection by DHS? If yes, please include a copy of the notice(s) with this PTA upon submission.	☒ Yes. Please describe. ☐ No. Please describe.

CBP One™ App Specific: Notice of the collection of PII will be provided to the user in the Terms and Conditions before entering the application. A copy of this document is provided with the submission of the PTA.

Functionality Specific: Additionally, the individuals collecting information on behalf of undocumented individuals and submitting this information to CBP, through CBP One™, are responsible for notifying the individual.

5. Disclosures

a) Does the mobile application provide "just-in- time"[10] 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. ☒ No. Please describe.

N/A, all information is submitted via the undocumented individual, or by another individual on behalf of the undocumented individual. The undocumented individual voluntarily submits their information to CBP or to the other individual (preparer) who then uploads the information into the CBP One™ mobile application.

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

N/A

6. Opt-out Features

a) Does the mobile application provide users with independent opt-out features[11] 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. ☒ No. Please describe.

Use of the CBP One™ mobile application is voluntary. Location-based services and the mobile device camera must be enabled by the user prior to launching this functionality. If the user opts-out to enabling their device camera or location-based services, they will be unable to continue through this functionality and sent back to the home screen of the app.

7. Mobile App-Specific Privacy Policy

a) Does the mobile application have an App-Specific Privacy Policy 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 upon submission.	☒Yes. Please describe. No. Please describe.

The Privacy Policy is listed in the application's Terms and Conditions. DHS approved a CBP One™ Mobile App Privacy Policy with the original submission of the CBP One™ PTA.

8. DHS Carwash process?

a) Has this mobile application been through the DHS Carwash[14] process?	□Yes. **Please provide the results of the arwash with this PTA.** No. Please describe.

CBP has conducted multiple AppVet scans on CBP One. CBP will conduct a new DHS AppVet after the May 23, 2022 deployment for this capability. CBP does no expect the results to be different from previous scans.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6), (b)(7)(C)
Date submitted to Component Privacy Office:	**May 02, 2022**
Date submitted to DHS Privacy Office:	May 4, 2022

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)

(b)(5)

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
Approved by:	(b)(6)
PRIVCATS Workflow Number:	**Click here to enter text.**
Date approved by DHS Privacy Office:	**May 17, 2022**
PTA Expiration Date	**May 17, 2023**

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/Privacy Notice required. ☐ Privacy Policy required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Specialized training required. ☐ Other. Click here to enter text.
PIA:	**New PIA is required.**

	• Forthcoming Collection of Advance Information from Certain Undocumented Individuals at the Land Border PIA. Further PIA coverage: • DHS/CBP/PIA-006(e) Automated Targeting System (ATS); • DHS/CBP/PIA-069 CBP One™ Mobile Application; • DHS/CBP/PIA-067 U.S. Customs and Border Protection, Unified Secondary; • DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing; • DHS/CBP/PIA-021 TECS System: Platform; and • DHS/CBP/PIA-056 Traveler Verification Service.
SORN:	**System covered by existing SORN** If covered by existing SORN, please list: • DHS/CBP-006 Automated Targeting System (ATS); and • DHS/CBP-011 U.S. Customs and Border Protection TECS.

DHS Privacy Office Comments: ***Please describe rationale for privacy compliance determination above.***

(b)(5)

Homeland
Security

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	**CBP One Mobile Application (Overarching PTA)**		
DHS Component:	Customs and Border Protection (CBP)	Office or Program	Office of Field Operations (OFO)/Planning, Program Analysis and Evaluation (PPAE)
Date of last PTA (if applicable):	N/A		
If pilot, pilot start date:	TBD	Pilot end date:	TBD

MOBILE APPLICATION DEVELOPMENT PROGRAM/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

OIT MOBILE APPLICATION DEVELOPMENT LEAD

Name:	(b)(6), (b)(7)(C)		
Office:	Office of Information and Technology	Title:	Supervisory IT Specialist
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

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.*

U.S. Customs and Border Protection (CBP), Office of Field Operations, is submitting this new PTA to document a new mobile application, CBP One, which will be the overarching platform/mobile application in which every CBP mobile application resides. The CBP One Mobile app itself does not collect any data, the app is intended to act as an intuitive single point of access to multiple CBP mobile application capabilities. The CBP One mobile application is available to members of the public through the IOS or Android app stores.

This PTA provides privacy compliance coverage for the CBP One Mobile Application only. Additionally, each CBP mobile applications residing in the CBP One Mobile application must have a separate PTA approved by DHS Privacy prior to adding the mobile application to the CBP One overarching platform/mobile application.

Accessing the CBP One Mobile App & CBP Privacy Policy:
The CBP One mobile application will prompt travelers to provide their Login.Gov credentials or register with the General Services Administration's (GSA's) Login.gov. In order to register with Login.gov, travelers have to provide an email address, a phone number, and create a password. Login.gov does not share any information provided by the user with CBP. Each time CBP One is launched by a traveler a notification displaying the CBP Privacy Policy will appear and individuals must consent to it prior to using the mobile application. Login.Gov ensures a secure connection and identity verification when using the CBP One mobile application.

CBP Mobile Applications Residing on CBP One:
The following mobile application have adjudicated PTAs from DHS and will reside within the CBP One environment:

1) CBP One Mobile App- Stakeholder Scheduling Functionality (PTA Adjudicated by DHS Privacy on 03/11/2020)
2) I-94/Exit Mobile (PTA adjudicated by DHS Privacy on 04/06/20, Renewal Required)

[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.

2. Subjects and Users[2] of the Mobile Application?

a. Who will SUBMIT information into this mobile application?	☒ Members of the public. ☐ DHS Employees ☐ DHS Contractors ☐ Other federal employees or contractors.
Members of the public will submit information into the CBP One Mobile App.	
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.
There is no information submitted into CBP One other than email address in order to log in. Each application within CBP One will collect information and that information will be used by DHS employees and members of the public. CBP will submit separate mobile app PTAs to cover those applications.	

3) Data to be received by CBP

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

The following information is collected from members of the public when creating a Login.gov account:

- **First name**
- **Last name**
- **Phone number**
- **Email address**
- **Login.gov password created by user**
- **Device ID (Mobile Phone ID)**

The email address collected when creating a Login.gov account, will be stored locally on the mobile device. The login.gov email address is stored only when the user is logged into the CBP One mobile app, and then immediately deleted after the session ends.

b) How is the information stored? *Please describe below.*	☒ Locally on the mobile device. ☐ In a backend CBP IT system. ☐ With a third party vendor. ☐ Other. Describe________

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

[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.

The login.gov user email will be stored locally on the mobile device. The login.gov user email will be encrypted on the mobile device. The login.gov email address is stored only when the user is logged into the CBP One mobile app, and then immediately deleted after the session ends.	
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 ☐ Other. Describe________ **N/A**
d) List the *specific authority* to collect SSN or these other sensitive PII elements	
N/A	
e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.	
N/A	
f) Does the mobile application collect other types of sensitive information[5]? Check all that apply.	☐ Location Information[6] ☐ 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.	
N/A	

4. Notices	
a) Are individuals provided notice[8] at the time of collection by DHS? If yes, please include a	☒ Yes. Please describe.

[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.

[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.

copy of the notice(s) with this PTA upon submission.	☐ No. Please describe.
Notice of the collection of PII will be provided to the user in the Privacy Policy before entering the application. A copy of this document is provided with the submission of the PTA. Additionally, each application within CBP One will have its own privacy policy.	

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. ☒ No. Please describe. The application does not use location services or the camera feature on mobile devices.
The user is presented with the Terms and Conditions which lists all PII or SPII before entry into the application. The application itself does not collect location data or require photos of any sort. As a result, asking for the user's permission to collect such information is not necessary. The Privacy Policy is listed in the application's Terms and Conditions. A copy is provided with the submission of this PTA.	
b) Does the mobile application provide any information to third parties (any organization outside of CBP)?	☐ Yes. Please describe. ☒ No. Please describe.
The application does not provide any information to parties outside of CBP. Applications within CBP One may provide information to third parties and that will be noted in their specific PTAs.	

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. ☒ No. Please describe. N/A
CBPOne as the shell application does not have services that can be opted out of. Applications within CBPOne may, and that will be noted in those PTAs.	

[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)

[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

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. ☐ No. Please describe.
The Privacy Policy is listed in the application's Terms and Conditions. A copy is provided with the submission of this PTA.	

8. DHS Carwash process?	
a) Has this mobile application been through the DHS Carwash[13] process?	☒ Yes. Please provide the results of the Carwash with this PTA. ☐ No. Please describe..
DHS AppVet results for android and iOS are attached to the 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:	**October 15, 2020**
Date submitted to DHS Privacy Office:	October 19, 2020
Component Privacy Office Recommendation:	

[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

[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.

Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.

(b)(5)

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:	October 26, 2020
PTA Expiration Date	October 26, 2023

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. Click here to enter text.
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: DHS/ALL/PIA-015 DHS Web Portals 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/ALL-004 General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792 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)

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One™ Mobile Application – Advance Information for Certain Undocumented Individuals in order to Seek Admission to the United States (Title 42 and Post Title 42)
DHS Component:	U.S. Customs and Border Protection (CBP) Office of Field Operations (OFO) Planning, Program Analysis, and Evaluation (PPA&E)
Date of last PTA:	N/A
If pilot, pilot start date:	N/A

MOBILE APPLICATION DEVELOPMENT PROGRAM/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	CBP/OFO/PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

Mobile App Specific-PTA QUESTIONS

1. Purpose of DHS Mobile Application

1) Describe the purpose of the DHS mobile application. *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.*

CBP Privacy is submitting this updated PTA to discuss updates to CBP One™, "Traveler" persona, "Land" section, "Submit Advance Information" tab in which certain undocumented individuals, can voluntarily submit biographic information, as well as a facial photograph, to CBP in advance of their arrival at a land Port of Entry (POE). This PTA was last adjudicated in May 2022. This PTA accounts for updates that occurred in January and May 2023.

January 2023

On January 12, 2023, CBP expanded the advance information submission functionality to certain undocumented individuals who seek to travel to the United States through southwest border (SWB) land POEs to request an exception to the Centers for Disease Control and Prevention (CDC) Order, "Suspending the Right to Introduce Certain Persons from Countries Where a Quarantinable Communicable Disease Exists (hereafter referred to as Title 42)."[1]

While the Title 42 Order is in effect, undocumented individuals seeking to travel to the United States through a SWB POE to request an exception to Title 42 must first use CBP One™ to attest that they believe that they or an accompanying spouse or child meet certain vulnerability criteria. After the individual attests that they believe that they, or their accompanying spouse or child meet the criteria, they are then able to submit advance information to CBP to request a date and time to present at an identified POE to request an exception to the Title 42 Order. Use of CBP One™ does not guarantee that an individual will be granted an exception to the Title 42 Order.

While the Title 42 Order is in effect, after the preferred language is selected, users will be presented with a list of the following vulnerability criteria:

- Physical or mental illness;

[1] On March 20, 2020, the Department of Health and Human Services (HHS) issued an Interim Final Rule (IFR) and Order under Sections 265 and 268 of Title 42 of the U.S. Code, which permits the Director of the Centers for Disease Control and Prevention (CDC) to "prohibit [...] the introduction" into the United States of individuals when the Director believes that "there is serious danger of the introduction of [a communicable] disease into the United States."9 Section 268 of Title 42 provides that customs officers—which include officers of CBP's Office of Field Operations and U.S. Border Patrol agents—shall implement any quarantine rule or regulation issued by the CDC, which includes Orders under section 265. The Order permits customs officers to except individuals from the CDC Order in totality of the circumstances based on "consideration of significant law enforcement, officer and public safety, humanitarian, and public health interests." On August 2, 2021, the CDC issued an updated *Suspending the Right to Introduce Certain Persons from Countries Where a Quarantinable Communicable Disease Exists, available at* https://www.cdc.gov/coronavirus/2019-ncov/cdcresponse/laws-regulations.html.

- Disability;
- Pregnancy;
- No access to safe housing or shelter in Mexico;
- Under the age of 21;
- Over the age of 70; or
- Have been threatened or harmed while in Mexico.

As part of this release, the individual was also offered the opportunity to schedule their desired arrival land POE location, date of arrival, and time of arrival.

May 2023 Update

With the termination of Title 42, CBP can no longer require undocumented individuals to attest to the vulnerability criteria in CBP One™, as described above. However, the Department of Homeland Security has issued a Notice of Proposed Rulemaking, titled Circumvention of Lawful Pathways, which will require many undocumented individuals to use CBP One™ in order to be eligible for asylum in the United States.[2] This rule will be made final prior to the end of Title 42 and CBP is making enhancements within CBP One™ to prepare.

In addition to the removal of the vulnerability criteria, CBP is making significant enhancements to the scheduling functionality within CBP One™. CBP One™ users and stakeholders continue to report frustration and stress, particularly related to a process that requires all users to access the app at the same time and attempt to get a limited number of appointments. Most importantly, CBP is concerned about the reports of potential fraud and exploitation related to the current process.

With this update, users will no longer be required to access the application at the same time each day to select a POE to see the availability of appointments. Instead, users will now be able to request an appointment once each day at the time that is best for them and then check to see if they were allocated an appointment (for 13 days later) the following day. CBP will use an algorithm to randomly allocate daily appointments to undocumented individuals who request an appointment each day. In the event an individual is not allocated an appointment, they must request an appointment again to be considered for the next day's allocation. Individuals who are offered an appointment are notified that they were allocated an appointment through an email notification, a push notification to the device that requested the appointment, an in-app message that will display when they access the app, and an update to their registration status within the CBP One™ application. After this notification is sent, the individual is given 23 hours to confirm the appointment by completing the photo capture and liveness detection process as described below.

With this update, CBP is now storing the latitude and longitude information for 1 year within the AWS CACE environment. This information is not associated with a specific device or individual. Instead, this information is used by CBP personnel to identify trends and potential vulnerabilities with CBP One™. Furthermore, this information is stored within the AWS CACE environment, separate from the personally identifiable information collected through CBP One™.

Background

.

[2] https://www.federalregister.gov/documents/2023/02/23/2023-03718/circumvention-of-lawful-pathways

Typically, once an undocumented individual arrives at a land POE for processing, CBP Officers (CBPOs) spend significant time collecting and verifying basic biographic data about the individual during the inspection process. One at a time, the CBPOs interview and collect information from such individuals during secondary inspection. The CBPOs manually enter the information into the Unified Secondary System (USEC).[3] To facilitate processing upon arrival and reduce the amount of manual data entry into primary and secondary processing systems, CBP One™ data will be displayed on the primary inspection screen and available for importation into secondary processing events.

Once the individual is logged in to CBP One™, they are prompted to select "Traveler", then "Land", then "Submit Advance Information". First time users will be prompted to select their preferred language (English or Spanish). After these steps are complete, the user must then select "Add Individual". CBP One™ then collects the same information that CBP would otherwise collect during the primary and/or secondary inspection, including:

- Facial photograph
- First and last name
- Date of birth
- Nationality
- Country/city of birth
- Country of residence
- Travel document information
- Phone numbers
- U.S. address
- Foreign addresses (optional)
- Employment history (optional)
- Travel history (optional)
- Emergency contact information (optional)
- Family information
- Martial information
- Identity documents (optional)
- Gender
- Height
- Weight
- Eye color

For individuals arriving with co-travelers, the process discussed above will need to be repeated, and CBP One™ will create a single submission for all co-travelers.

CBP One ™ will also collect latitude and longitude coordinates. These coordinates will be sent to CBP

[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE UNIFIED SECONDARY, DHS/CBP/PIA-067, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

to determine whether the submission is occurring within 30 miles of the U.S.- Mexico border. All undocumented individuals submitting information through CBP One ™ are required to be within 30 miles of the U.S.-Mexico border (as determined by the phone's GPS at the time of submission) and must complete liveness detection through their device's camera prior to scheduling a presentation date at a POE. In addition, CBP One™ collects the preparer's (person assisting the individual with their submission) first and last name and email address.

After the data is submitted, the individual is presented with a confirmation screen which displays a confirmation number along with the selected POE and date/time, if applicable. In addition, a confirmation email will be sent to the email address(es) provided under contact information during the CBP One™ submission, or, in the absence of an email within CBP One™, it will be sent to the registered email of the Login.gov account.

Prior to arrival at the POE, CBP may use the information submitted by the individual to conduct system checks to identify individuals who may pose a risk to national security, border security or public safety. These checks are identical to the checks conducted by CBP during the primary or, in some cases, secondary inspection process.[4] CBP will not inform the user of the outcome of these checks, but CBPOs will use the information during primary and secondary inspections.

During primary inspection at the POE, the CBPO will use the Simplified Arrival system to take a new facial photograph.[5] This facial photograph will search against multiple CBP Traveler Verification Service (TVS) galleries including a pre-staged "Submit Advance Information" gallery. The "Submit Advance Information" gallery consists of templates that CBP created from the facial photograph submitted by users during the submission process. If there is a match, the information the user submitted through CBP One™, as well as the results of the system checks, will be displayed to the CBPO. If no match is made, CBPOs will manually enter the individual's confirmation number or biographic data to populate Simplified Arrival for processing in primary. As with any individual who arrives at the POE without documentation, the CBPO will use Simplified Arrival to create a referral to secondary for further processing, to include the confirmation number received from CBP One™. Once referred to secondary, CBP Officers may import the information captured through the CBP One™ application into a USEC event.

CBP has published a standalone PIA titled "Collection of Advance Information from Certain Undocumented Individuals on the Land Border" to more fully explain CBP's collection of information from undocumented individuals in advance of their arrival at POE.

[4] *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.

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE – APPENDIX A ON SIMPLIFIED ARRIVAL, DHS/CBP/PIA-056, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

2. Subjects and Users 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.

Certain Undocumented individuals can voluntarily submit biographic information, as well as a facial photograph, to CBP in advance of their arrival at a land Port of Entry (POE). This information is submitted through the CBP One App.

Additionally, individuals (family members or co-travelers) on behalf of undocumented individuals may submit information into this mobile application.

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 Officers (CBPOs) who conduct primary and secondary inspections at Ports of Entry. Pre-arrival vetting information will be used to streamline and expedite CBPOs' processing of individuals, including identifying those who may pose a security threat.

3) Data to be received by CBP

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

CBP One™ collects the same information that CBP would otherwise collect during the primary and/or secondary inspection, including:

- Facial photograph
- First and last name
- Date of birth
- Nationality
- Country/city of birth
- Country of residence
- Travel document information
- Phone numbers
- U.S. address
- Foreign addresses (optional)
- Employment history (optional)
- Travel history (optional)
- Emergency contact information (optional)

- Family information
- Martial information
- Identity documents (optional)
- Gender
- Height
- Weight
- Eye color

For individuals arriving with co-travelers, the process discussed above will need to be repeated, and CBP One™ will create a single submission for all co-travelers. CBP One ™ will also collect latitude and longitude coordinates. These coordinates will be sent to CBP to determine whether the submission is occurring within 30 miles of the U.S.- Mexico border. In addition, CBP One™ collects the preparer (person assisting the individual with their submission)'s first and last name and email address.

b) How is the information stored? *Please describe below.*	☒ Locally on the mobile device. ☒ In a backend CBP IT system. ☐ With a third-party vendor. ☐ Other. Describe________

No PII information is stored locally on the undocumented individual or representative's device or in the CBP One application itself. CBP pushes all information collected through CBP One™ to back-end systems. Individuals submitting directly will have their confirmation number and scheduled POE, day and time saved to their device. The retention of information CBP collects through CBP One™ depends on the respective CBP One™ service.

CBP temporarily retains the photographs of undocumented individuals within TVS for 1 year for identity confirmation, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. Furthermore, the advance information, including the photograph, that is collected via CBP One is stored in a segregated database within ATS for 1 year. Upon arrival and once the advance information is imported into a USEC event and verified, or a UPAX event is created during pre-arrival vetting, the information will be stored within ATS for 15 years consistent with the ATS retention schedule. In addition, the USEC event data will be transmitted into and stored in other systems, where it will be retained in accordance with the retention schedules for those systems. For example, information that is sent to and stored in TECS is retained for 75 years in accordance with the TECS retention schedule. Many of the forms completed through USEC are sent to the U.S. Immigration and Customs Enforcement (ICE) Enforcement Integrated Database (EID) as the source system, in which case they are stored for 75 years.[6]

c) Does the mobile application collect Social Security number (SSN) or	☐ Social Security number

[6] EID is a DHS shared common database repository used by several DHS law enforcement and homeland security applications. EID stores and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, U.S. Citizenship and Immigration Services (USCIS), and CBP. EID supports ICE's processing and removal of noncitizens from the United States. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacydocuments-ice.

other elements of Sensitive Personally Identifiable Information (SPII)? Check all that apply.	□ Alien Number (A-Number) X Passport Number □ Bank Account, Credit Card, or other financial account number (via pay.gov) □ Other. Describe: Biographic data (see 3a)

d) List the *specific authority* to collect SSN or these other sensitive PII elements

The following CBP legal authorities permit the collection of border crossing information: Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638; Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354; Aviation and Transportation Security Act of 2001 (ATSA); Enhanced Border Security and Visa Reform Act of 2002.

e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

This information collection is required to streamline processing at the Port of Entry.

f) Does the mobile application collect other types of sensitive information? Check all that apply.	□ Location Information[7] ☒ Photos/Videos ☒ Mobile Device ID ☒ Metadata □ Other. Describe________ Device ID/Metadata - This information is collected by CBP One™ as a whole. This action is performed at log in. This is used for other capabilities for push notification. We do not use this data for this use case, but there is no way to turn on and off based on capability.

g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.

Liveness Photos are collected to verify identification once an individual arrives at a POE. All undocumented individuals submitting information through CBP One ™ must complete liveness detection through their device's camera prior to scheduling a presentation date at a POE.

4. Notices

a) Are individuals provided notice[9] at the time of collection by DHS? If yes, please include a copy of the notice(s) with this PTA upon submission.	☒ Yes. Please describe. ☐ No. Please describe.

CBP One™ App Specific: Notice of the collection of PII will be provided to the user in the Terms and Conditions before entering the application. A copy of this document is provided with the submission of the PTA.

Functionality Specific: Additionally, the individuals collecting information on behalf of undocumented individuals and submitting this information to CBP, through CBP One™, are responsible for notifying the individual.

5. Disclosures

a) Does the mobile application provide "just-in- time"[10] 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. ☒ No. Please describe.

N/A, all information is submitted via the undocumented individual, or by another individual on behalf of the undocumented individual. The undocumented individual voluntarily submits their information to CBP or to the other individual (preparer) who then uploads the information into the CBP One™ mobile application.

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

N/A

6. Opt-out Features

a) Does the mobile application provide users with independent opt-out features[11] 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. ☒ No. Please describe.

Use of the CBP One™ mobile application is voluntary. Location-based services and the mobile device camera must be enabled by the user prior to launching this functionality. If the user opts-out to enabling their device camera or location-based services, they will be unable to continue through this functionality and sent back to the home screen of the app.

7. Mobile App-Specific Privacy Policy

a) Does the mobile application have an App-Specific Privacy Policy 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 upon submission.	☒Yes. Please describe. No. Please describe.

The Privacy Policy is listed in the application's Terms and Conditions. DHS approved a CBP One™ Mobile App Privacy Policy with the original submission of the CBP One™ PTA.

8. DHS Carwash process?

a) Has this mobile application been through the DHS Carwash[14] process?	☒Yes. **Please provide the results of the arwash with this PTA.** No. Please describe.

CBP has conducted multiple AppVet scans on CBP One. CBP will conduct a new DHS AppVet after the May 23, 2022 deployment for this capability. CBP does no expect the results to be different from previous scans.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6), (b)(7)(C)
Date submitted to Component Privacy Office:	**May 2, 2023**
Date submitted to DHS Privacy Office:	May 2, 2023

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)

Homeland Security

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)
Approved by:	(b)(6)
PRIVCATS Workflow Number:	0014391
Date approved by DHS Privacy Office:	**August 2, 2023**
PTA Expiration Date	**August 2, 2026**

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/Privacy Notice required. ☐ Privacy Policy required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Specialized training required. ☐ Other. Click here to enter text.
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: DHS/CBP/PIA-068 CBP One™ Mobile Application; DHS/CBP/PIA-076 Collection of Advance Information from Certain Undocumented Individuals at the Land Border: Post Title 42; DHS/CBP/PIA-009(a) – TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative; DHS/CBP/PIA-021 TECS System: Platform
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

DHS Privacy Office Comments: ***Please describe rationale for privacy compliance determination above.***

(b)(5)

(b)(5)

Homeland Security

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One Mobile Application- Advance Information for Undocumented Individuals		
DHS Component:	Customs and Border Protection (CBP)	Office or Program	OFO/PPAE
Date of last PTA (if applicable):	April 22, 2021		
If pilot, pilot start date:	Click here to enter a date.	Pilot end date:	Click here to enter a date.

MOBILE APPLICATION DEVELOPMENT PROGRAM/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	CBP/OFO	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

OIT MOBILE APPLICATION DEVELOPMENT LEAD

Name:	(b)(6), (b)(7)(C)		
Office:	CBP/OIT	Title:	Supervisory IT Specialist
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

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.*

U.S. Customs and Border Protection (CBP), Office of Field Operations (OFO) is submitting this new PTA to discuss the continued use of the CBP One Mobile Application to include advance information to aid in the processing of undocumented individuals who are not subject to the Migrant Protection Protocols (MPP) after the current Centers for Disease Control and Prevention (CDC) Order suspending certain noncitizens from entering the United States at or near the land border during the COVID19 pandemic is rescinded. In addition, this PTA specifically identifies the individual's ability to input advance information into the CBP One app on their own behalf without the assistance of an International Organization or Non-Government Organization.

Similar to the current non-MPP collection, all information from this new population of individuals will be collected on a voluntary basis and submitted to CBP via the CBP One Mobile or web application. Application.

Background

On March 20, 2020, the Department of Health and Human Services (HHS) issued an Interim Final Rule (IFR) and Order under Sections 265 and 268 of Title 42 of the U.S. Code, which permits the Director of the CDC to "prohibit ... the introduction" into the United States of individuals when the Director believes that "there is serious danger of the introduction of [a communicable] disease into the United States." Section 268 of Title 42 provides that customs officers—which includes officers of U.S. Customs and Border Protection (CBP)'s Office of Field Operations and Border Patrol agents—shall implement any quarantine rule or regulation issued by the CDC, which includes Orders under section 265. The CDC Order issued on March 20, 2020 has been extended and amended. The most current version of the Order was issued on October 13, 2020, after HHS issued a Final Rule (FR) under Sections 265 and 268 of Title 42 of the U.S. Code. The CDC Order does not apply to U.S. citizens, lawful permanent residents, and their spouses and children, nor does it apply to U.S. military personnel or those who arrive at a port of entry with valid travel documents. The Order also includes an exception for anyone whom customs officers determine should be allowed into the United States on "consideration of significant law enforcement, officer and public safety, humanitarian, and public health interests."

[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.

To streamline the processing at ports of entry of certain individuals who may be determined to be excepted from the Order based on humanitarian interests, CBP leveraged the existing CBP One Mobile Application information collection functionality. CBP One was initially deployed in February 2021 to verify the identity and eligibility of individuals enrolled in the Migrant Protection Protocol program. DHS adjudicated the PTA for the MPP CBP One use case on February 10, 2021. Additionally, CBP documented the CBP One MPP use case in an Appendix to the CBP One PIA. On April 22, 2021, a PTA entitled "CBP One Mobile Application - NGO Functionality for non-MPP enrollee" was approved to expand this collection to facilitate orderly processing of undocumented individuals, amenable for processing under the discretionary humanitarian exception to the CDC Order.

Process for Undocumented Individuals

Irrespective of a CDC order, undocumented individuals, on their own or through a IO/NGO, will continue utilize CBP One to voluntarily submit their biographic information, as well as their photograph, prior to their arrival at a CBP POE for processing. This is a change from submission only being permitted by IO/NGOs.

This advance information collection will significantly streamline Title 8 processing at the POE. Typically, once an individual arrives to the POE for Title 8 processing, CBP Officers (CBPOs) spend significant time collecting and verifying basic biographic data about undocumented individuals during the inspection process. One at a time, the CBPOs interview and collect information from individuals during secondary inspection. The CBPOs manually enter the information into the Unified Secondary System (USEC). To facilitate processing upon arrival and reduce the amount of manual data entry into secondary processing systems, CBP One data will be available for importation into secondary processing events.

Undocumented individuals may provide this information prior to arrival to CBP via the CBP One mobile or web-based application. While no information is stored locally in the CBP One mobile nor web-based application or on a user's device, this data is stored in a segregated backend database within the Automated Targeting System (ATS). The information will be tagged as coming from CBP One. CBP will store a templatized copy of the picture in a standalone Traveler Verification Service (TVS) gallery to be matched against a photograph taken by a CBPO once the individual arrives at the POE using Simplified Arrival.

The TVS gallery will be built off the new backend dataset ingesting into ATS specifically for the non-MPP population. If any photos are submitted to ATS from CBP One, the new TVS gallery will stage those photos until they arrive at the POE. Using Simplified Arrival, once an undocumented individual arrives at the POE, CBP will take a new photograph to search against the new non-MPP gallery within TVS. If no match is made, CBPOs will manually query ATS based on biographic data to populate Simplified Arrival for processing in primary. As with any individual who arrives at the POE without documentation, the CBPO will use Simplified Arrival to create a referral to secondary for further processing, to include the confirmation number received from CBP One. Once referred to secondary, CBP Officers may import the information captured through the CBP One application into a USEC event.

This will reduce the time spent manually entering data, in primary and secondary. In secondary, the officers will review the advanced data collected for accuracy, edit the data and save the information in USEC event.

The overall goal of the program is to achieve efficiencies to process individuals under Title 8 consistent with public health protocols, and space limitations. When data is collected in advance, it helps expedite the secondary processing because it will reduce manual data entry into the USEC event, which reduces subject time in congregate settings.

Pre-vetting

Prior to arrival at the POE, CBP will also use the information to conduct system checks to identify individuals that may pose a risk to national security, border security or public safety. These system checks will also streamline processing for individuals processed under Title 8.

Data Storage & Retention

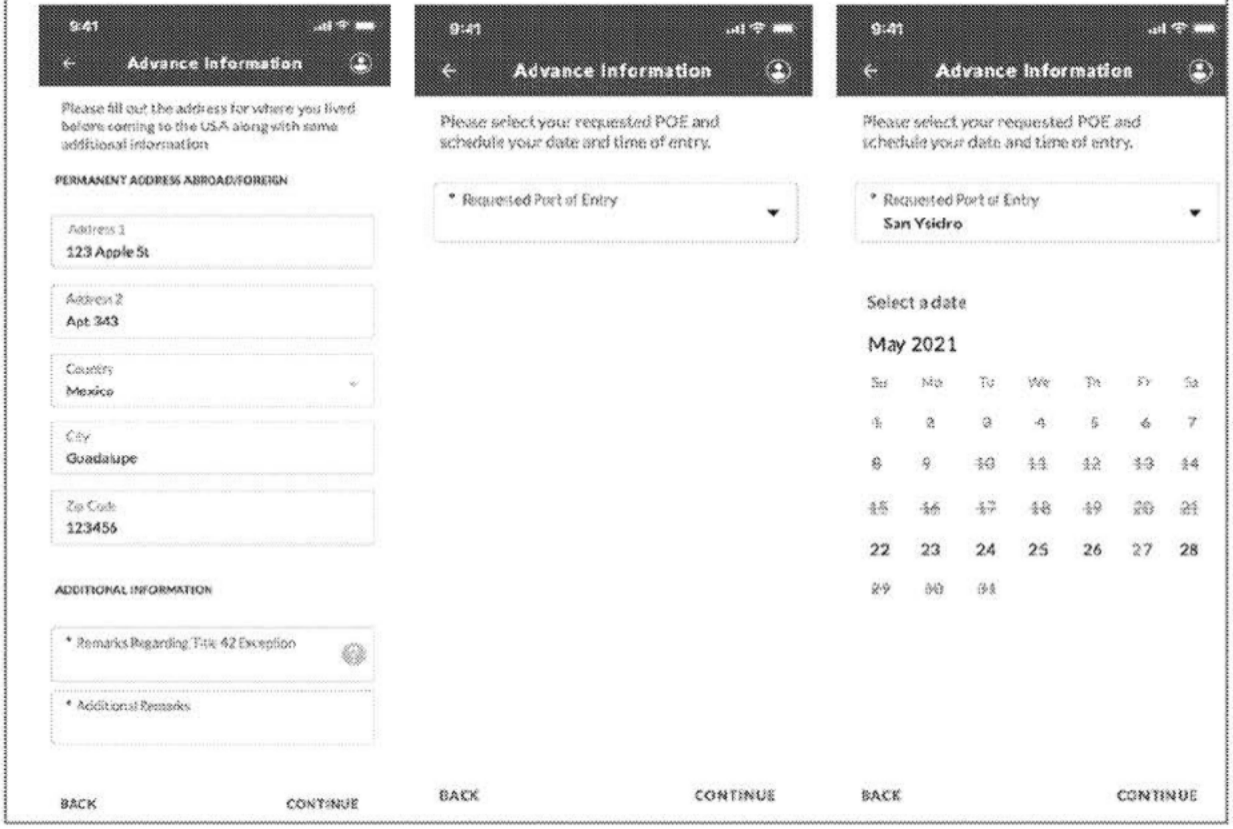
No information is stored locally on the user's device or the web-based application. All new information will be stored in a segregated database within the Unified Secondary backend tables and will be used to run system checks in advance of the expected arrival at the POE, as well as to pre-populate the Unified Secondary event upon arrival at the POE in order to expedite the Secondary processing. CBP is also conducting an updated USEC PTA and PIA to describe this process in full.

The data will also be retrievable by CBP employees in the Office of Information Technology in order to provide CBP leadership with anonymized statistics related to workload and record location ability. For example, number of submissions, citizenship, age range, and expected port of arrival.

Querying and Selecting Available Times at the POE

CBP is also updating CBP One to permit Undocumented individuals the ability to schedule an appointment date/time , in which they would appear in person for CBP processing at a land a POE. This functionality will be available at the end of the Non-MPP workflow, after the user inputs their permanent address abroad foreign and any additional title 42 information. Users will be prompted to select a POE and a calendar will be displayed in the app. The user must then select a date in the calendar. ***Note: the user will only have the option to select a date that is within a 7-day window. All other dates will be strike out on the calendar.*** The available time slots will display based on the date selected. If there are no time slots available on the selected date for the group, verbiage will display asking the user to select another date. Once confirmed, this information will be provided to the individuals on the confirmation page within the CBP One app and in their confirmation email. The confirmation page in the CBP One app will display a green check mark and confirmation number to the individual. Individuals should save this confirmation number for future reference. The individuals will also have the ability to enter their confirmation number and retrieve their current scheduled day and time for the ATS backend. They can then select a new day and time based on availability and receive a new confirmation. No PII will be retrieved using the confirmation number.

Non-MPP > Scheduling an appt



Please fill out the address for where you lived before coming to the USA along with some additional information

PERMANENT ADDRESS ABROAD/FOREIGN

Address 1
123 Apple St

Address 2
Apt 343

Country
Mexico

City
Guadalupe

Zip Code
123456

ADDITIONAL INFORMATION

* Remarks Regarding Title 42 Exception

* Additional Remarks

Please select your requested POE and schedule your date and time of entry.

* Requested Port of Entry

Please select your requested POE and schedule your date and time of entry.

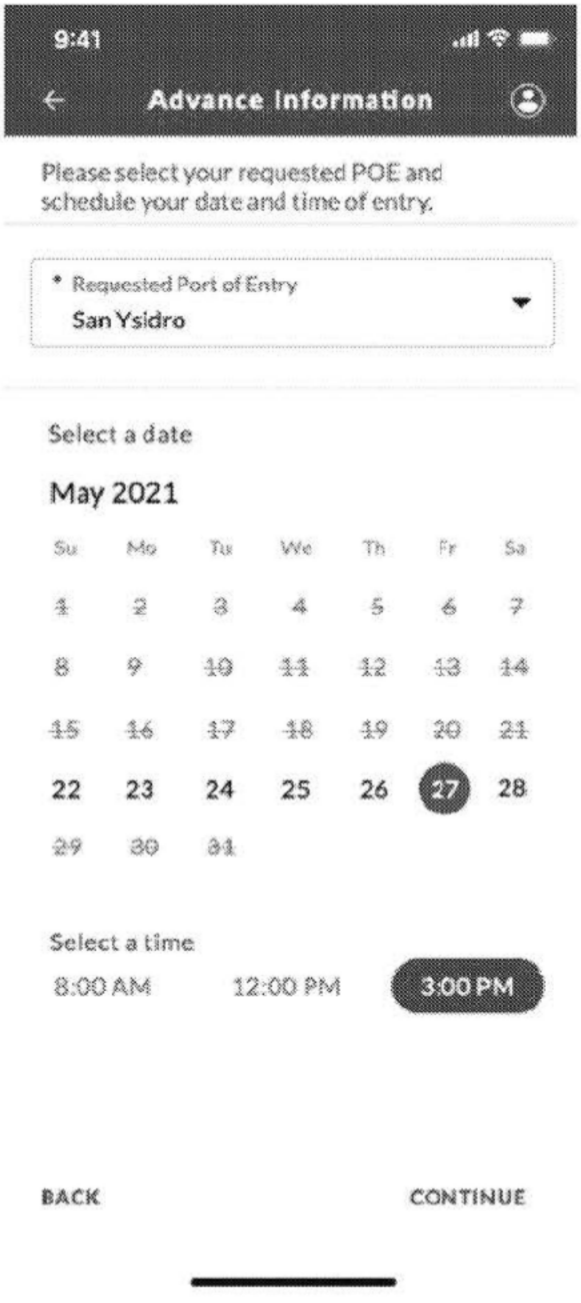
* Requested Port of Entry
San Ysidro

Select a date

May 2021

Su	Mo	Tu	We	Th	Fr	Sa
~~1~~	~~2~~	~~3~~	~~4~~	5	6	7
~~8~~	~~9~~	~~10~~	~~11~~	~~12~~	~~13~~	~~14~~
~~15~~	~~16~~	~~17~~	~~18~~	~~19~~	~~20~~	~~21~~
22	23	24	25	26	27	28
29	30	31				

Non-MPP > Scheduling an appt



9:41

Advance Information

Please select your requested POE and schedule your date and time of entry.

* Requested Port of Entry
San Ysidro

Select a date

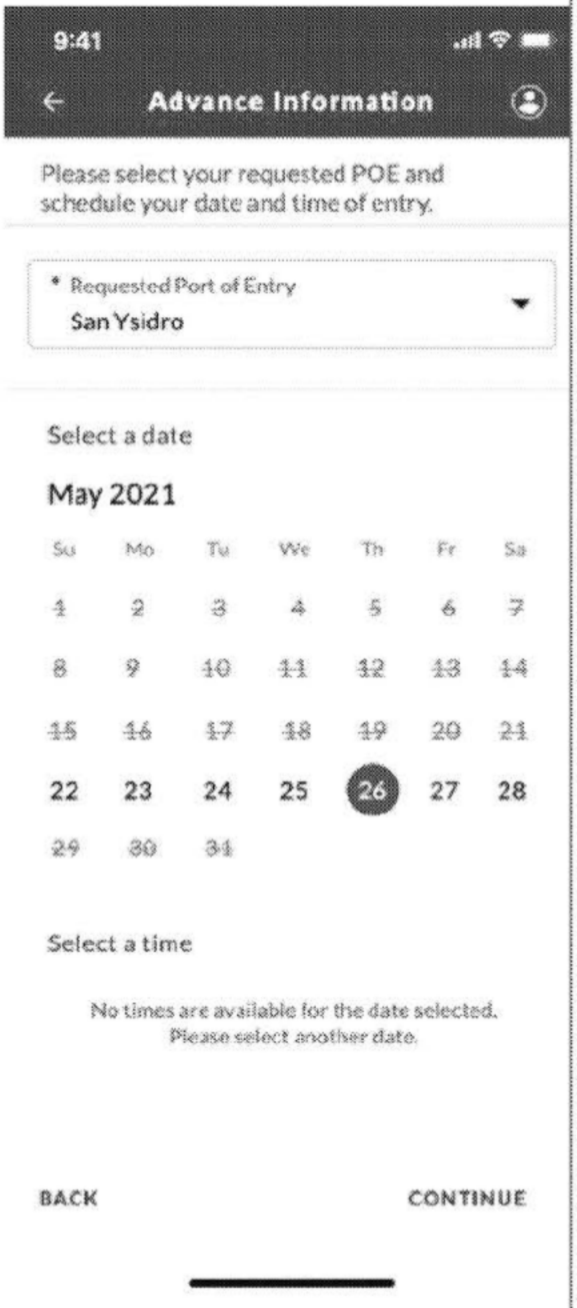
May 2021

Su	Mo	Tu	We	Th	Fr	Sa
~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~
~~8~~	~~9~~	~~10~~	~~11~~	~~12~~	~~13~~	~~14~~
~~15~~	~~16~~	~~17~~	~~18~~	~~19~~	~~20~~	~~21~~
22	23	24	25	26	27	28
~~29~~	~~30~~	~~31~~				

Select a time

8:00 AM 12:00 PM 3:00 PM

BACK CONTINUE



9:41

Advance Information

Please select your requested POE and schedule your date and time of entry.

* Requested Port of Entry
San Ysidro

Select a date

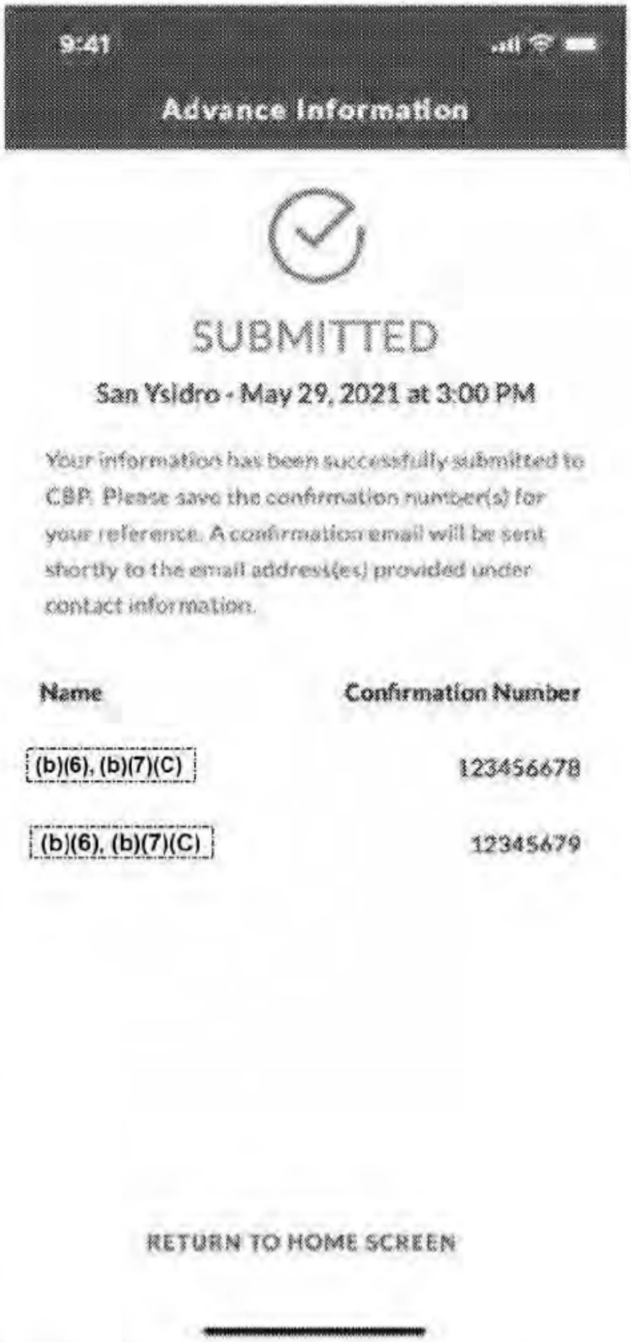
May 2021

Su	Mo	Tu	We	Th	Fr	Sa
~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~
~~8~~	~~9~~	~~10~~	~~11~~	~~12~~	~~13~~	~~14~~
~~15~~	~~16~~	~~17~~	~~18~~	~~19~~	~~20~~	~~21~~
22	23	24	25	26	27	28
~~29~~	~~30~~	~~31~~				

Select a time

No times are available for the date selected.
Please select another date.

BACK CONTINUE



9:41

Advance Information

SUBMITTED

San Ysidro - May 29, 2021 at 3:00 PM

Your information has been successfully submitted to CBP. Please save the confirmation number(s) for your reference. A confirmation email will be sent shortly to the email address(es) provided under contact information.

Name	Confirmation Number
(b)(6), (b)(7)(C)	123456678
(b)(6), (b)(7)(C)	12345679

2. Subjects and Users[2] of the Mobile Application?

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

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.
Undocumented Individuals will submit information into CBP One.	
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 Officers who conduct primary and secondary inspections at Ports of Entry. Pre-arrival vetting information will be used to streamline and expedite CBPOs' processing of individuals, including identifying those who may pose a security threat.	

3) Data to be received by CBP

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

Biographic or other data includes, but is not limited to descriptive information such as:

- Name (required)
- Data of birth (required)
- Contact Information (required)
- Addresses (required)
- Nationality (required)
- Employment history (required)
- Travel history (required)
- Emergency Contact (optional)
- U.S. and foreign addresses (required)
- Familial Information (optional)
- Marital Status (optional)
- Identity Document (not a WHTI compliant document) (optional)
- Gender (required)
- Preferred Language (required)
- Requested Port of Entry (required)
- Requested Date and Time of Entry (required)

CBP notes that these fields mirror the existing information collection for the I-94W.

Biometric data includes, but is not limited to descriptive information such as:

[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.

- Height (required)
- Weight (required)
- Eye color (required)
- Photograph (optional)

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________

No information is stored locally on the user's device. All new information will be stored in a segregated database within the backend Unified Secondary system and will be used to run system checks in advance of the expected arrival at the Port of Entry, as well as to pre-populate the Unified Secondary event upon arrival at the POE in order to expedite the Secondary processing.

CBP is also conducting an updated USEC PTA and PIA to describe this process in full.

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) X Passport Number ☐ Bank Account, Credit Card, or other financial account number ☐ Other. Describe________

d) List the *specific authority* to collect SSN or these other sensitive PII elements

The following CBP legal authorities permit the collection of border crossing information: Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638; Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354; Aviation and Transportation Security Act of 2001 (ATSA); Enhanced Border Security and Visa Reform Act of 2002.

e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

This information collection is required to streamline processing at the Port of Entry.

[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.

f) Does the mobile application collect other types of sensitive information[5]? Check all that apply.	☐ Location Information[6] X Photos/Videos X Mobile Device ID X Metadata[7] ☐ Other. Describe________ This information is collected by CBP One as a whole. This action is performed at log in. This is used for other capabilities for push notification. We do not use this data for non-MPP but there is no way to turn on and off based on capability.
g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.	
Photos are collected to verify identification once an individual arrives at a POE.	

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.
Undocumented individuals will use CBP One™ to submit advance information to CBP. Notice of the collection of PII will be provided to the user in the Terms and Conditions before entering the application. A copy of this document is provided with the submission of the PTA.	

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)?	x Yes. Please describe. ☐ No. Please describe.

[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.

[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)

The mobile app asks to access the user's device camera for pictorial submission.	
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.
Location-based services and additional app capabilities are not available for this functionality; therefore there is nothing the user can customize or opt-out of. All information submitted is strictly voluntarily.	

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.	X Yes. Please describe. ☐ No. Please describe.
The Privacy Policy is listed in the application's Terms and Conditions. DHS approved a CBP One Mobile App Privacy Policy with the original submission of the CBP One PTA.	

8. DHS Carwash process?

[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

a) Has this mobile application been through the DHS Carwash[13] process?	☐ Yes. Please provide the results of the Carwash with this PTA. X No. Please describe.
The CBP One Mobile Application regularly submits functionality via the DHS AppVet process; the last scan was on March 25, 2021 to include all previously approved functions. The traveler functionality will be submitted through the DHS AppVet scan once functional.	

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6), (b)(7)(C)
Date submitted to Component Privacy Office:	**May 25, 2021**
Date submitted to DHS Privacy Office:	Click here to enter a date.
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 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 1, 2021
PTA Expiration Date	

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. **Updated Privacy Policy**
PIA:	**New PIA is required.** Advance Information for Processing Undocumented Individuals If covered by existing PIA, please list: Click here to enter text. If a PIA update is required, please list: DHS/CBP/PIA-068 CBP One Mobile Application
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; DHS/CBP-016 Nonimmigrant Information System, March 13, 2015, 80 FR 13398 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)

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application:	**CBP One Mobile Application- Scheduling Functionality Renewal**		
DHS Component:	**Customs and Border Protection (CBP)**	Office or Program:	**Office of Field Operations (OFO), Planning, Program Analysis and Evaluation (PPAE)**
Launch date:	Click here to enter a date.	Project or program status:	**Operational**
Date of last PTA (if applicable):	**June 17, 2021**		

MOBILE APP DEVELOPMENT PROGRAM MANAGER/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	OFO/PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

MOBILE APP DEVELOPMENT LEAD/INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	(b)(6), (b)(7)(C)		
Office:	Office of Information and Technology (OIT)	Title:	Supervisory IT Specialist
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

Mobile App Specific-PTA QUESTIONS

1. Purpose of DHS Mobile Application

Describe the DHS mobile application[1]. *Please provide a general description of the mobile app and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades that are triggering the update to this PTA. If this is a renewal PTA, please state whether or not there were any changes to the mobile app since the last version.*

U.S. Customs and Border Protection (CBP), Office of Field Operations (OFO) is submitting this renewal PTA for the scheduling functionality embedded into CBP One™. There have been no changes since the last PTA (adjudicated on June 17, 2021).

CBP One Login & Privacy Policy

CBP One™ is available for Android and iOS mobile devices in the Google Play or iTunes mobile application stores. Users must create a new or open an existing Login.Gov account in order to access CBP One™. CBP uses Login.gov to manage users' authentication by allowing users to sign in with an email address, password, multi-factor method, and conduct identity proofing by verifying the individual's asserted identity. To register with Login.gov, users must provide an email address and a phone number and create a password. Login.gov does not share any information provided by the user with CBP. The mobile app will ask the user to enable push notifications upon the first time opening the CBP One ™, and logging into the mobile application. Each time a user launches CBP One™, a notification displaying the CBP Privacy Policy will appear, and users must consent to it prior to using the mobile application.

Once the user has logged in via Login.gov and consented to the privacy policy, the landing page will launch which permits the user to select from different options that describe the individual's reason for using CBP One™. CBP One™ will display different functions based on the user's selections. For some functions, users can input information for themselves, as well as for others. This makes it easier for groups to submit information and streamlines CBP's vetting and inspection processes.

Currently, CBP One™ is available for brokers/carriers/forwarders to make appointments for the inspection of perishable cargo by accessing the scheduling functionality. The scheduling functionality embedded into the CBP One™ Mobile application, is an optional tool for use by stakeholders to assist with processing of their cargo at the ports.

Scheduling Functionality

The scheduling functionality provides a mobile and web option for brokers, carriers, and forwarders to quickly request a cargo inspection appointment for commercial vessels or cargo entering the United States, view real time appointment status updates, view inspection request history, and interact with a CBPAS via a chat feature embedded into the mobile and desktop application. The scheduling functionality reduces unnecessary wait time for runners, enhances

[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. For more information, please see DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

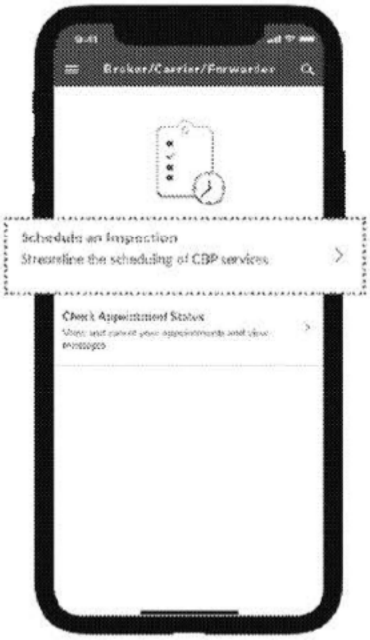
communication between CBP and the broker/carrier/forwarder, and streamlines the inspection process at POE.

Schedule an Inspection

Once the broker/carrier/forwarder (user) has logged into Login.gov, they will be directed to the CBP One mobile application "Who Are You" page and the user must then select "broker/carrier/forwarder" persona to enter the scheduling functionality. The user will then be prompted to enter the following data fields into the mobile app: Company Name; Group Email; Port; First Name; and Last Name. Once the user enters this information into the mobile application, they will be directed to the "Broker/Carrier/Forwarder" screen and can either select "Schedule an Inspection" or "Check an Appointment Status".

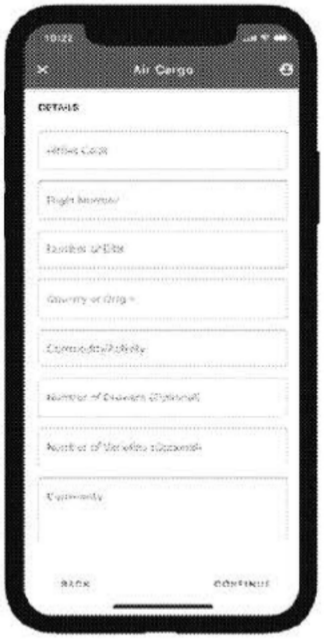
If the user selects "Schedule an Inspection" they must then select the appointment/inspection type, "Perishable Cargo". The user must then select the cargo type (e.g., Air Cargo, Land Cargo, or Sea Cargo). Presently, only the "Air Cargo" option is active in the CBP One App. OFO plans to launch the Land and Sea Cargo options soon. Once the user selects "Air Cargo", they will then be prompted to enter the following information: Airline Code; Flight Number; Airway Bill Number; Number of Bills, Country of Origin, Commodity/Activity; Number of Growers (Optional); Number of Varieties (Optional); and Comments. The user will then be directed to the "Schedule Inspection" page. Here the user can add a point of contact on-site and must enter the following information: First Name; Last Name; Phone Number. The app will then prompt the user to enter the following inspection information: Date; Port; Location or Site Location; Number of Boxes for Inspection; Time your inspection will be ready; and are overtime expenses authorized? (Yes or No). If the user selects "No" to the overtime question, they must then select "Submit" at the bottom of the screen and the information will be sent to CBP. The mobile app will display a green check mark notification that reads "Inspection Requested". If the user selects "Yes" to the overtime question, the user will be directed to enter the following importer ID information: Company; and Importer ID Number. Once this information is entered, the user can then select "Submit" and the information will be sent to CBP. The mobile app will display a green check mark notification that reads "Inspection Requested".

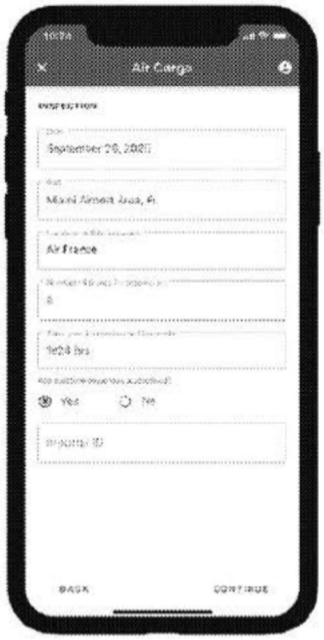
A CBPO/CBPA will then access the scheduling dashboard to review and confirm the appointment. The user will then receive in app and push notifications, along with emails on the status of their appointment. A CBP Agriculture Specialist (CBPAS) may then initiate a chat which the user can respond to under the "Conversation Tab".



Schedule an Inspection
Streamline the scheduling of CBP services

Check Appointment Status





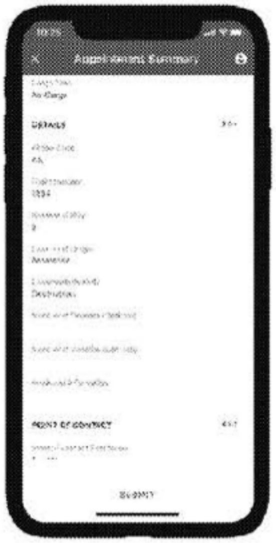
September 29, 2021

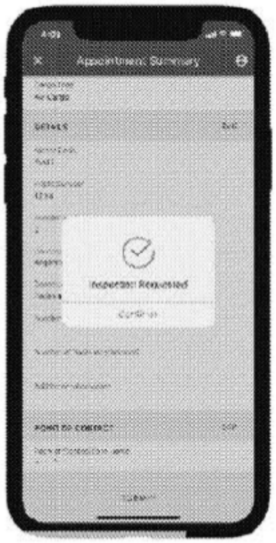
Miami Airport Area, FL

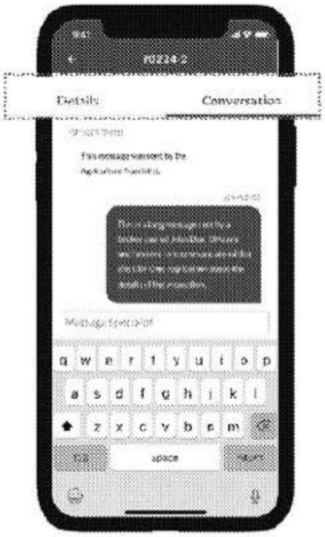
Air France

1624 lbs

● Yes ○ No



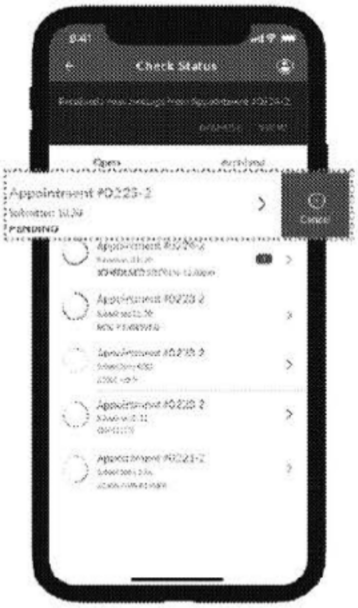




This message was sent to the Agriculture Specialist.

View/Cancel/Edit an Inspection

If the user wants view/edit details on their inspection or check their appointment status they can select the "Check Appointment Status" tab, and all of their active appointments will appear. If the user needs to cancel an inspection, they can simply swipe to the left on the screen or click on the "Cancel Appointment" button in the details tab. *All Completed/Cancelled appointments will be achieved. Only pending inspections can be edited, while pending, acknowledged, doc reviewed, and assigned inspections can be cancelled.*



Check Status

Open

Appointment #0223-2
Submitted: 10.26
PENDING

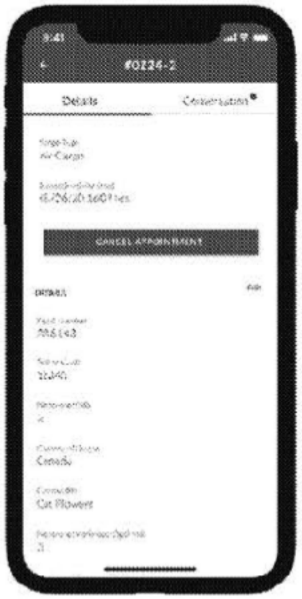
Cancel

Appointment #0223-2

Appointment #0223-2

Appointment #0220-2

Appointment #0221-2



#0224-2

Details

Conversation

Air Cargo

CANCEL APPOINTMENT

Canada

Cut Flowers

Storage of Information

Users will have to provide basic biographic information, such as first and last name, contact information, and email address, to create a Login.gov account and use the application. Profile creation is done through Login.gov, and CBP One, as an umbrella application, does not store information on users.

In addition, the CBP One™ mobile app does not store any information locally on the device. CBP pushes all information collected through the CBP One™ mobile app, Scheduling functionality, to the CBP Scheduling Dashboard. This information is stored in a CBP backend database within the CACE environment. CBP One Mobile Application, Scheduling Functionality, records are covered under N1-36-86-1/162/12: Cargo Examination and Inspection Records. Retention: Temporary. Destroy when no longer required for administrative needs.

The CBP Scheduling Dashboard will automatically purge data older than 365 days. The CBP Scheduling Dashboard does not send any data to the CBP One Mobile app, nor does it connect to any other internal or external systems.

CBP Scheduling Dashboard

The CBP Scheduling Dashboard, is a standalone web application that resides on the CACE environment, and is accessible to CBP employees, and CBP contractors via a computer workstation, laptop, or tablet. The CBP Scheduling Dashboard provides an avenue for CBPAS to view inspection requests and assign inspection times. CBPAS can also use the CBP Scheduling Dashboard to communicate with the broker/carrier/forwarder (members of the public). CBP Supervisory employees and CBP employees also use the dashboard to communicate internally between each other in matters related to the inspection process. Brokers/Carriers/Forwarders who do not have access to a mobile device (cellphone or tablet) can use the CBP One web application to quickly request a cargo inspection appointment for commercial vessels or cargo entering the United States, view real time appointment status updates, view inspection request history, and interact with a CBPAS via a chat feature.

The CBP Scheduling Dashboard will directly connect to and support the CBP One mobile app. The CBP Scheduling Dashboard ingests, and stores data generated through use of the CBP One mobile app. The CBP Scheduling Dashboard will automatically purge data older than 365 days. The CBP Scheduling Dashboard does not send any data to the CBP One Mobile app, nor does it connect to any other internal or external systems.

2. Subjects and Users[2] of the Mobile Application Information

a. Who will SUBMIT information into this mobile application? *Please describe below, including what Components if it involves DHS personnel.*	☒ Members of the public ☒ DHS personnel ☐ Other federal employees

Private business stakeholders (brokers/carriers/forwarders) will use the mobile app to request a cargo inspection appointment for commercial vessels or cargo entering the United States, view real time appointment status updates, view inspection request history, and interact with a CBPAS via a chat feature embedded into the mobile and desktop application.

CBPAS use the Scheduling Dashboard to view inspection requests, assign inspection times, and to communicate with the broker/carrier/forwarder (members of the public).

b. Who will USE the information submitted to DHS from this mobile application? *Please describe below, including what Components if it involves DHS personnel.*	☐ Members of the public ☒ DHS personnel ☐ Other federal employees

CBP employees will use the information submitted through CBP One, scheduling functionality, to schedule inspection appointments, and communicate with brokers/carriers/forwarders.

3) Data to be collected

a) What information will be submitted through the mobile application? *Please list all data elements.*

All Stakeholders (brokers/carriers/forwarders): Company/Individual name; Point of Contact first and last name (for companies); phone number; e-mail address; conveyance type; inspection type; number of bills; airway bill number; country of origin; commodity type; number of varieties; number of growers; date of inspection; location of inspection; port; location or site location; number of boxes for inspection; time inspection will be ready; overtime expenses authorized; an additional information

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

field; conveyance information; vessel name; registration country; conveyance arrival; itinerary; any special permit requests (per 19 CFR PART 4), and mobile device ID

Importers only: Importer ID (provided by CBP)

Private Travelers only: Passport document number; import permit number; issuing agency for permit, and Document Imaging System (DIS) transaction number.

b) Does the mobile application collect Sensitive Personally Identifiable Information (SPII)?[3] 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 ☐ DHS Electronic Data Interchange Personal Identifier (EDIPI) ☐ Social Media Handle/ID ☐ Known Traveler Number/Other Traveler ID Number ☐ Driver's License Number ☐ Biometrics (e.g., fingerprints, facial images/photographs) X Other. Please list: **Importer ID (used in some cases where overtime is requested)**

c) List the *specific authority* to collect SSN or these other SPII elements. *Note*: even if the program is properly authorized to collect SSNs, you are required to use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking/truncating the SSN, or blocking the display of SSNs within the mobile application.[4]

The following CBP legal authorities permit the collection of border crossing information: Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638; Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354; Aviation and Transportation Security Act of 2001 (ATSA); Enhanced Border Security and Visa Reform Act of 2002; and Tariff Act of 1930 as amended, 19 U.S.C. 66, 1433, 1459, 1485, 1624, and 2071.

d) Describe *why* this collection of SPII is necessary and the minimum amount of information required to accomplish the purpose of the program.

[3] DHS defines Sensitive Personally Identifiable Information (SPII) as 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.

[4] Please see DHS Instruction Number: 047-01-009 (Social Security Number Collection and Use Reduction).

A private traveler's passport number is needed to verify the traveler's identification when completing an inspection. Passport information will rarely be collected; only when the application's user is a traveler hand carrying sensitive agricultural items via air carrier and needs to notify CBP that an inspection will be required upon arrival.

e) Does the mobile application collect other types of sensitive content information?[5] Check all that apply.	☐ Location Information[6] ☐ Photos/Videos[7] X Mobile Device ID ☐ Metadata[8] ☐ Other. Please list:

f) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.

The Mobile Device ID is required for push notifications which will provide status updates for the requested inspections and will notify the user of incoming chat messages sent by the CBP Agricultural Specialists. The goal would be to keep the user abreast of the status of submitted inspection requests. The users can disable notifications through their respective devices as opposed to in the application itself.

g) How and where is the information stored? *Please describe below.*	☐ Locally on the mobile device X In a back-end DHS system ________________ ☐ With a third-party vendor ☐ Other. Describe________

h) How long is information stored or retained? If the data is stored in multiple places, please provide the information for all locations. *Please describe below and indicate retention schedules if applicable.*

Users will have to provide basic biographic information, such as first and last name, contact information, and email address, in order to create a Login.gov account and use the application. Profile creation is done through Login.gov, and CBP One, as an umbrella application, does not store information on users.

In addition, the CBP One™ mobile app does not store any information locally on the device. CBP pushes all information collected through the CBP One™ mobile app, Scheduling functionality, to the CBP Scheduling Dashboard. This information is stored in a CBP backend database within the CACE environment. CBP One Mobile Application, Scheduling Functionality, records are covered

[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] Photos/videos meaning the mobile app access the device's camera or photo library.

[8] 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.

under N1-36-86-1/162/12: Cargo Examination and Inspection Records. Retention: Temporary. Destroy when no longer required for administrative needs.

The CBP Scheduling Dashboard does not send any data to the CBP One Mobile app, nor does it connect to any other internal or external systems.

i) How do you ensure that information is disposed of or deleted in accordance with the retention schedule?	
The CBP Scheduling Dashboard will automatically purge data older than 365 days.	
j) Does the project, program, or system retrieve information by personal identifier?	X Yes. Please list personal identifiers below. ☐ No.
Yes, the users email address is used by the overarching CBP One application to retrieve information about the user profile.	

4. Notices

a) Are individuals provided a Privacy Act Statement, Privacy Notice, or some, other type of notice[9] 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.
Once the user has logged in via Login.gov, they will be prompted to consent to the CBP One™ Mobile Application privacy policy. Once the user provides their consent the landing page will launch which permits the user to select from different options that describe the individual's reason for using CBP One™. CBP One™ will display different functions based on the user's selections. The Scheduling functionality will require its own privacy policy and the draft is attached to this PTA submission.	

5. Disclosures

a) Does the mobile application provide "just-in-time"[10] 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.
The user is presented with the Terms and Conditions which lists all PII or SPII before entry into the application. The application does not collect location data or require photos of any sort. As a result, asking for the user's permission to collect such information is not necessary.	

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

[10] 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 other DHS Components or systems?	☐ Yes. Please describe. X No.
The application does not provide any information to other DHS Components or systems.	
c) Does the mobile application provide any information to third parties (any organization outside of DHS)?	☐ Yes. Please describe. X No.
The application does not provide any information to parties outside of CBP.	

6. Opt-out Features

a) Does the mobile application provide users with independent opt-out features[11] 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.
There are no services from which to opt-out. Users can choose to opt-out from notifications via their respective devices.	
b) Before allowing a user to submit information to DHS, does the mobile application provide a "review before sending" function that allows users to correct or opt-out of sending their information to the Department?	☐ Yes. Please describe. X No.
N/A	

7. Mobile App-Specific Privacy Policy

a) Does the mobile application have an App-Specific Privacy Policy[12] 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 upon submission.	X Yes. Please describe. ☐ No.
CBP One App has it's own privacy policy.	

8. DHS AppVet process?

[11] 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.

[12] All DHS Mobile apps are required to have a Privacy Policy that is easily accessible to users through the commercial app store before installation as well as within the app, itself, after installation. This Privacy Policy should be app-specific and cannot merely reference the DHS website Privacy Policy. For more information, please see DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

a) Has this mobile application been through the DHS AppVet[13] process?	X Yes. **Please provide the results of the AppVet with this PTA.** ☐ No.
The CBP One Mobile Application regularly submits functionality via the DHS AppVet process; the last scan was on May 19, 2022 to include all previously approved functions. This application will be run through the DHS AppVet process before June 3rd and the results will be shared with DHS Privacy.	

[13] DHS AppVet is the service sponsored by DHS Office of the Chief Technology Officer (OCTO) 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 AppVet also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility. DHS AppVet replaced the DHS Carwash. This is a requirement of DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

PRIVACY THRESHOLD REVIEW
(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6), (b)(7)(C)
Date submitted to Component Privacy Office:	**May 24, 2022**
Date submitted to DHS Privacy Office:	May 24, 2022
Concurrence from other Components involved (if applicable):	N/A

(b)(5)

(b)(5)

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
DHS Privacy Office Approver (if applicable):	(b)(6)
PCTS Workflow Number:	(b)(6)
Date approved by DHS Privacy Office:	May 24, 2022
PTA Expiration Date	May 24, 2024

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/Privacy Notice required. ☐ Privacy Policy required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Specialized training required. ☐ Other. Click here to enter text.
e(3)/ Privacy Notice	Choose an item.
Privacy Policy	Choose an item.
PIA:	**PIA update is required.** If covered by existing PIA, please list: • DHS/CBP/PIA-068 CBP One Mobile Application – **update required**
SORN:	**System covered by existing SORN** If covered by existing SORN, please list: • DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792 • DHS/CBP-001 Import Information System, July 26, 2016, 81 FR 48826

DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*
(b)(5)

(b)(5)

Homeland Security

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One™ Mobile Application, Bus Operator Functionality		
DHS Component:	Customs and Border Protection (CBP)	Office or Program PPAE/STO	
Date of last PTA (if applicable):	**N/A**		
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: OFO/PPAE		Title: Director STO
Phone: (b)(6), (b)(7)(C)		Email: (b)(6), (b)(7)(C)

OIT MOBILE APPLICATION DEVELOPMENT LEAD

Name:	(b)(6), (b)(7)(C)		
Office:	CBP/OIT	Title:	Management and Program Analyst
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

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.*

History

Previously, CBP submitted a PTA titled "Reporting Offsite Arrival Mobile Application (ROAM), Land Pre-Arrival System (LPAS) functionality" (which expired on September 27, 2020), which described the manifest submission functionality of CBP ROAM, called LPAS. LPAS provided bus and rail carriers, entering the United States, a mobile option to submit an APIS manifest and carrier information to CBP prior to crossing a U.S. land border. CBP is submitting this new PTA to document the migration of the LPAS bus manifest functionality. the LPAS bus manifest functionality will migrate to the CBP One™ Mobile Application (Mobile App). Additionally, the ROAM LPAS functionality PTA also discussed the rail functionality, which is still embedded into the CBP ROAM mobile application. At this time there are no plans to migrate the rail functionality to the CBP One Mobile App.

Overview and Process Steps

Bus carriers can use either eAPIS or the CBP One Mobile App to voluntarily submit bus manifest information to CBP prior to arriving at a POE. eAPIS is a CBP web-based computer application that collects traveler manifest information from commercial carriers for international travel both into and out of the United States. eAPIS is discussed in further detail in the eAPIS Cloud PTA (adjudicated 10/17/2018), and the TECS APIS PTA (adjudicated 01/13/2021). CBP receives very limited submissions of Advanced Passenger Information (API) through eAPIS. Also, information received is often inaccurate and CBP cannot accurately assess the treat risk of individuals entering the United States.

CBP One Mobile App provides users a mobile option to submit advanced information to CBP. CBP One™, is available for bus operators and bus company personnel through their smart device (via the Apple App Store or Google Play Store). Bus carriers and/or bus company personnel can choose to enter and submit bus manifest data into CBP One.

CBP One™ profile creation is done through Login.gov, which ensures a secure connection and identity verification for CBP One™ users. In order to register with Login.gov, users have to provide an email address and a phone number and create a password. Login.gov does not share any information provided by the user with CBP. Each time a user launches CBP One™, a notification displaying the CBP Privacy Policy will appear and users must consent to it prior to using the mobile application.

Once the user has logged in via Login.gov and consented to the privacy policy, the landing page will launch which permits the user to select from different options that describe the individual's

[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.

reason for using CBP One™. In order to access this functionality in the CBP One Mobile App, bus carriers must select the "bus operator" option from the landing page.

Once the user accesses the CBP One- Bus Operator Functionality, they will be prompted to enter their assigned carrier code and sender ID. CBP issues both the carrier code and sender ID to bus carriers. Both codes are unique identifiers and are used to identify the bus carrier company in APIS. The carrier code and sender ID are an additional layer of security used to authenticate the bus carrier employee into CBP One-Bus Operator Functionality. These two fields only manifest themselves when logged into the CBP One- Bus Operator functionality. Without the carrier code and sender ID, the bus carrier employee cannot access the Bus Operator Functionality.

After the bus operator is authenticated through CBP One, they will be directed to provide data on the bus. The user is prompted to provide biographic and trip information manually into the submission screen or they can use their phones camera to Machine Readable Zone (MRZ) scan the passengers Western Hemisphere Travel Initiative (WHTI)-compliant document to populate the biographic information into the travel document text fields of the submission screen. Once the bus operator has scanned the MRZ of all passengers WHTI-compliance document or manually entered their biographic information (if necessary) into CBP One™, the bus operator will be prompted to submit the manifest to CBP. *Note: The photo on the travel document will be collected during the MRZ scan. However, the image is deleted upon submission to CBP and is not viewed by CBP Officers.*

Once the data is submitted through the mobile application, law enforcement checks are completed from the CBP system and an APIS manifest is created. CBP Officers (CBPOs) will then review the APIS manifest and conduct enhanced checks as needed. In addition, CBPOs use the information submitted through the CBP One Mobile App to conduct targeting queries and review passengers in advance of their arrival at the land border. Once a traveler arrives at the Port of Entry, CBPOs will utilize Simplified Arrival (SA) or mobile primary to process the traveler and match them to the data submitted to APIS through CBP One ™.

Note: The information collected through the CBP One Mobile App, Privacy Notice, and Retention are discussed below in questions 3a, 3b, and 4.

Additional Information

CBP uses Hyper Text Transfer Protocol Secure (HTTPS) to securely transfer the traveler(s) document information and trip itinerary from their personal device via Wi-Fi or cellular service, to the Amazon Web Services (AWS) Cloud database, which is securely partitioned using the AWS Cloud. Once CBP receives the traveler(s) and trip information, CBP conducts automated biographic queries against backend law enforcement databases, such as the TECS System and the National Criminal Information Center (NCIC) in the same manner as if a traveler presented him or herself at the POE. Additionally, data is compiled in the Advanced Passenger Information System (APIS) developing a APIS manifest for CBP advanced query functionality.

2. Subjects and Users[2] of the Mobile Application?

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

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.
Bus operators and bus company personnel	
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 (CBPOs)	

3) Data to be received by CBP

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

Bus operators can voluntarily submit their bus manifests selecting "Bus Operator" in the CBP One™ Mobile App. CBP will collect passenger APIS data through the application. This includes passenger and carrier details.

Bus Information

- License Country
- Registration state/province
- License number
- APIS Sender ID (provided by CBP to the bus carrier)
- APIS carrier code (provided by CBP to the bus carrier)
- Bus Company name

Arrival Details

- Arrival location in the U.S.
- Departure date of trip
- Departure time of trip
- Arrival date to the U.S.
- Arrival time to the U.S. Port of Entry
- Port of Entry arriving to
- State of Arrival
- Last Country Visited
- Contact email/phone number for bus operator

[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.

Traveler Information

- Scan document or manual entry of WHITI document info: first and last name; date of birth; gender; country of citizenship; country of residence; document type; document number; date of issue; date of expiration; country of issue; trusted traveler (All WHTI compliant documents), phone number.

Mobile Device Information

CBP will collect the below information from the bus operator's mobile device through CBP One™

- Device Type
- Device id
- Operating system version
- Phone model

b) How is the information stored?	x Locally on the mobile device. x In a backend CBP IT system. ☐ With a third party vendor. ☐ Other. Describe________

Retention Information:

All trip and biographic data collected from the bus driver and travelers through the user's mobile device will be deleted after submission to CBP, or after 24 hours from collection if the information was never submitted to CBP.

The carrier code and sender ID collected from the bus driver and submitted through the CBP One- Bus Operator Functionality, is sent to CBP APIS and will be written into the APIS manifest. This happens at the time of submission. Additionally, at the time of submission the carrier code and sender ID are immediately erased from CBP One.

All mobile device information collected (e.g., Device Type, Device ID, Operating System Version, and Phone Model) is retained for 365 days in the CBP one database.

All data, except for the mobile device information (listed above), will submitted through CBP One™ will be forwarded immediately to the Advance Passenger Information System (APIS) and will not be retained in the CBP One™ AWS cloud. APIS data is used for entry screening purposes and is retained for no more than 12 months. Data obtained through APIS is copied to BCI during the process of vetting an individual traveler or crew member and will be retained in accordance with the record retention period for BCI. If an individual is required to go through secondary inspection or some other enforcement action is taken, the inspection details will be maintained in TECS pursuant to that retention schedule.

All Login.gov records are stored electronically in a database in GSA's virtual cloud environment. All Login.gov records will be maintained for at least six years in accordance with NARA General Records Schedule (GRS) 3.2 "System access records," which covers user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges to partner agencies for usage of Login.gov. However, GSA is authorized to maintain the information for longer if it is required for business use.

CBP One™ – Mobile Application, Bus Operator Functionality, generates records that are covered under GRS 5.2, item 020. Intermediary records. Retention: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. APIS is the system of record for the passenger manifests that are submitted through the CBP One™ Mobile App.

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) **X** Passport Number ☐ Bank Account, Credit Card, or other financial account number **X** Other. Passport card, NEXUS card, Global Entry card, Sentri Card, Fast Card, Permanent resident card, Enhanced U.S. Driver's license (All WHTI Compliant Documents)

d) List the *specific authority* to collect SSN or these other sensitive PII elements

8 U.S.C. § 1101, The Immigration and Nationality Act

- Defies Alien Number and subsequent border crossing identification cards

8 U.S.C. § 1221., List of Alien and Citizen Passengers Arriving and Departing

- Inspection, Apprehension, Examination, Exclusion, and Removal
- Describes arrival and departure manifest as well as their contents to include passport or alien number

[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.

19 U.S.C § 1434, Penalties for violations of arrival, reporting, entry, and clearance requirements.

e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

APIS requires passenger manifest information that includes SPII such as Alien Number or Passport Number. Officers use this information to authorize entrance into the U.S. based on their standard operating procedures.

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.

The image of the passenger from their presented documentation is captured as a part of a routine MRZ scan of travel documents by CBP One™. Carriers utilize the application to capture passenger information based on identification presented. This image is not transmitted nor is it saved on the CBP backend systems.

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.

Bus passengers do not use the CBP One™ Mobile App, Bus Operator function and a DHS/CBP privacy notice is not provided to bus passengers via CBP One™. Passenger information is collected by the bus carrier.

Bus passengers traveling on bus carriers headed for a U.S. Port of Entry, must provide travel documentation to the bus carrier at or before arriving at the U.S. Port of Entry. Passengers cannot opt-out of this requirement and carriers may request this information be present at the time of the trip departure or at the time of the ticket purchase. Once the bus operator has logged in via Login.gov, they will be prompted to consent to the CBP One™ Mobile Application privacy policy.

[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.

Once the bus operator provides their consent the landing page will launch which permits the bus operator to select from different options that describe the operators reason for using CBP One™.

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)?	X Yes. Please describe. ☐ No. Please describe.

The bus operator is informed during CBP One Mobile App launch that this is an official system and that they are accepting the terms and conditions. Additionally, the bus operator is informed via the CBP One Privacy Policy, which appears after the individual signs into the CBP One Mobile Application.

Users are unable to utilize the CBP One Mobile App, unless they agree to a Privacy Policy set forth by Login.gov. Users have to acknowledge and accept the conditions prior to entering their Login.gov information. The Login.gov Privacy Policy is located at: **https://www.login.gov/policy/**

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

The CBP One Mobile Application does not provide any information to parties outside of DHS.

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.

No Opt-out services are appropriate for the use case of this mobile application.

The DHS/CBP/PIA-001(h)-Advanced Passenger Information System (APIS): Land Pre-Arrival System (LPAS) for bus and rail PIA, mentions the use of a geofencing feature and that users must enable their location services prior to entering information into LPAS. The CBP One Mobile

[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)

[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

Application-Bus Operator Functionality, will not use a geofencing feature and users will not need to enable location services prior to using the bus operator functionality.

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.	**X** Yes. Please describe. ☐ No. Please describe.
Yes, CBP One has an overarching Privacy Policy. The user must consent to Privacy Policy on the landing page, prior to moving forward through the mobile application.	

8. DHS Carwash process?	
a) Has this mobile application been through the DHS Carwash[13] process?	**X** Yes. **Please provide the results of the DHS AppVet process with this PTA.** ☐ No. Please describe.
Yes, the DHS AppVet process documents have been attached to this PTA.	

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:	**August 10, 2021**
Date submitted to DHS Privacy Office:	August 11, 2021

[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

[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.

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)

(b)(5)

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:	September 3, 2021
PTA Expiration Date	September 3, 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. Click here to enter text.
PIA:	**PIA update is required.** If covered by existing PIA, please list: DHS/CBP/PIA-021 TECS; DHS/CBP/PIA-006 Automated Targeting System If a PIA update is required, please list: DHS/CBP/PIA-001 Advance Passenger Information System (APIS); DHS/CBP/PIA-068 CBP One Mobile Application (appendix update)
SORN:	**System covered by existing SORN** If covered by existing SORN, please list: DHS/CBP-005 Advance Passenger Information System (APIS), March 13, 2015, 80 FR 13407; 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)

Homeland Security

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One Mobile Application- NGO Functionality		
DHS Component:	Customs and Border Protection (CBP)	Office or Program	Planning, Program Analysis and Evaluation (PPAE)
Date of last PTA (if applicable):	**January 22, 2021**	(addendum to the CBP One PTA)	
If pilot, pilot start date:	Click here to enter a date.	Pilot end date:	Click here to enter a date.

MOBILE APPLICATION DEVELOPMENT PROGRAM/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	OFO/PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

OIT MOBILE APPLICATION DEVELOPMENT LEAD

Name:	(b)(6), (b)(7)(C)		
Office:	Office of Information Technology	Title:	Supervisory IT Specialist
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

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.*

Background

In early 2019, CBP began implementing the Migrant Protection Protocol (MPP), which was a U.S. government action whereby certain foreign individuals, without proper documentation, entering or seeking admission to the United States from Mexico are returned to Mexico to wait outside of the United States for the duration of their immigration proceedings. In January 2021, the United States ended the MPP process and began the process of permitting foreign individuals previously in MPP to be processed into the United States. CBP estimates that around 25,000 individuals are currently enrolled in MPP and are now eligible to wait in the United States while their immigration case is proceeding. In order to enroll individuals in MPP, CBP used Unified Secondary and e3 to collect a photograph and biographic information from the individual. CBP stores this information in a CBP database in the Enforcement Integrated Database (EID). A separate PTA has been submitted to DHS which discusses the MPP program in detail.

CBP has formed partnerships with Non-Governmental Organizations (NGOs) on the ground in foreign countries to collect information from migrants and individuals who intend to migrant into the United States. CBP is submitting this new PTA to document a new use case of the CBP One Mobile Application. NGOs will now be able to submit biometric and biographic information on undocumented individuals into the mobile application and verify the Migrant Protection Protocols (MPP) Program enrollment. This use case will be on February 19, 2021 at the following U.S. land Ports of Entries (PoEs): San Ysidro, El Paso, and Brownsville. CBP will continue to work with NGOs as MPP enrollees are processed into the United States and to locate future asylum seekers.

CBP One Login

CBP is working with Non-Governmental Organizations (NGO), identified by the State Department, to verify individuals enrolled in MPP without a final immigration adjudication to streamline their processing into the United States. Individuals working for an NGO will download and access CBP One™ in the same manner as all other users of CBP One™. CBP will determine whether a user can have access to NGO functions in CBP One™ based on the information the user inputs to create a login.gov account. Eligible NGOs will provide email domain names to CBP and CBP will open access to the NGO functionality within CBP One™ to users who created login.gov accounts using that email domain. For example the American Red Cross, an NGO, may give CBP their email domain as @redcross.org, CBP would then allow any user who created a login.gov account using a @redcross.org email to view the NGO functionalities.

[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.

Once a user has access to the NGO functionality in CBP One™ they will be able to use the application to determine individuals that are enrolled in MPP and have an active immigration proceeding (no final adjudication).

NGO Process Steps
The undocumented individual capability will either (1) confirm individuals were previously encountered by CBP, enrolled in the MPP program, have not received a final disposition of their immigration case and returned to Mexico to wait for their immigration proceedings or (2) automate the manual process of CBP collecting required information and documentation in preparation for processing undocumented individuals not previously encountered by CBP PRIOR to entering the United States. Each part will be described separately below.

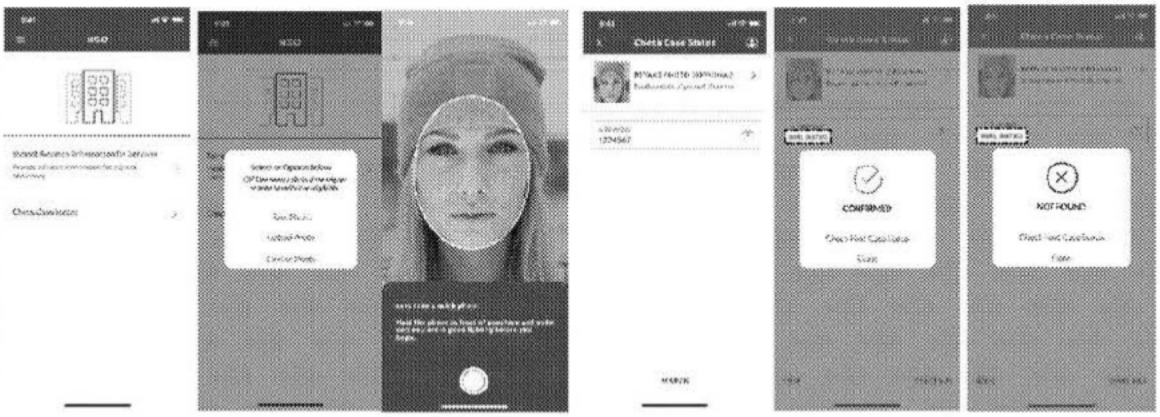
Part One: Confirming Individuals Previous Encounters
The MPPs are a U.S. Government (USG) action whereby citizens and nationals of countries other than Mexico arriving in the United States by land from Mexico -- whether or not at a Port of Entry (POE) -- may be returned to Mexico pursuant to Section 235(b)(2)(C) of the Immigration and Nationality Act (INA) while their U.S. removal proceedings are pending under Section 240 of the INA. The Government of Mexico, with NGO support, has committed to provide undocumented individuals placed into MPP with appropriate humanitarian protections, including immigration documentation and access to education, healthcare and employment.

Once a user has access to the NGO functionality in CBP One™ they will be able to use the application to determine if individuals are enrolled in MPP, and if they have an active immigration proceeding (i.e. with no final adjudication). To do this, an NGO user will take or upload an existing photograph of the individual into CBP One™. Once the user submits the information, CBP One™ will attempt to match the image against a pre-staged Traveler Verification Service (TVS) 2 gallery that is populated with all of the images from the MPP EID database. If a match is made, CBP will send the biographic information associated with the EID image to the U.S. Citizenship and Immigration Services' (USCIS) Person Centric Query System (PCQS) to verify that the individual still has a pending immigration case. Individuals with a final immigration adjudication are not eligible to continue with MPP processing. Once both the EID and PCQS search are complete, CBP sends a response back to the NGO CBP One™ user which is either a green check mark or a red "X". A green check mark indicates that the individual, whose picture the user submitted to CBP, is enrolled in MPP and has an active immigration case. A red "X" means they are not.

If they receive a red "X" the NGO can submit an alien identification number (A-number). Additionally, the NGO user can select a "decline to provide" button when asked to provide a photograph of the individual which will allow the NGO user to submit the individual's A-number. The A-number query will be sent to EID and PCQS to try and locate information in those systems associated with the A-number. Like with the photograph submission, based on the record located CBP then sends a response back to the NGO CBP One™ user with either a green check mark or a red "X". If the NGO receives another red "X", the final option will be to collect biographic information (name and date of birth) from the individual using CBP One™. The biographic information is also submitted to EID and PCQS

[2] TVS PIA

to locate matching records. As with the previous queries, CBP then sends a response back to the NGO CBP One™ user with either a green check mark or a red "X". If an individual is confirmed as enrolled in MPP and no final disposition of immigration proceedings, the NGO will work with CBP and the individual to set up a time for the individual to be presented to a Port of Entry for processing. The screenshots below show the different screens associated with Part One.



Part Two: Individuals not currently in MPP Program

NGOs would support the collection of advance entry data to expedite Non-MPP individual processing once they arrive at a CBP Port of Entry for processing. Typically, once they arrive the POE, CBP Officers (CBPOs) spend significant time collecting and verifying data on the undocumented individuals. The CBPOs provide the individuals a paper copy of an excel spreadsheet with questions. The individuals complete the information by hand. The CBPOs then review the information with the individuals and then manually enter the information into the Unified Secondary System (USEC).

The new CBP One capability will allow undocumented travelers to provide the same information via a mobile or desktop application electronically before their arrival at a POE. This data will be stored in the Amazon Web Services Cloud Service (CACE).

With this new simplified service, once an undocumented traveler arrives at the POE, their photo will be taken (if the POE has simplified arrival) or biographic data manually queried (if the POE uses Vehicle Primary Client (VPC)) to retrieve their information from CACE to populate the appropriate primary system. The primary system will initiate the event in USEC and refer the undocumented individual to secondary for further processing. Once in secondary, the officers will query the USEC event, review the accuracy of the data, edit the data to ensure accuracy and save the information in the USEC system.

The overall goal of this capability is to either confirm individuals who claim to be a part of MPP (for part one) or automate the data input into USEC (for part two) which will result in undocumented individuals being processed more quickly and efficiently so they spend less time in CBP custody. This will also allow CBP to increase capacity and process more individuals each day.

Data

NGOs will support migrants in submitting the following data points by either directly providing devices to migrants, or (in a smaller subset of cases) by assisting migrants using the migrants' own mobile devices.

Part One: Potential MPP Participants: photo and alien registration number

Part Two: Name, birthdate, place of birth, citizenship, height, weight, hair color, eye color, picture, travel documentation (i.e., passport number, document number), language preference, social media information, employment status (i.e., employed, employers number),family status, traveling status (i.e., are you alone, who are you traveling with), marital status, spouse information (i.e., name, birthdate, place of birth, citizenship), in-law information (for each in-law: i.e., name, birthdate, place of birth, citizenship), children information (for each child: i.e., name, birthdate, place of birth, citizenship), intended port of arrival, address information abroad (i.e., street, city, state, zip code, telephone), USA point of contact (i.e., name, relation, street address, city, state, zip code, telephone number).

The CBP One App functionality will interact with the following systems to perform pre-verification and validation: (b)(7)(E)

Data Storage & Retention

No information is stored locally on the user's device. CBP does not store the photo but will store the A-number and biographic data, if provided, in a CBP Amazon Web Services Cloud Service (CACE) database for 365 days. This data will be retrievable by CBP employees in the Office of Information Technology in order to provide CBP leadership with anonymized statistics related to workload and record location ability For example, number of submissions, number that required submitting the A-number and biographic data.

Audit

The CBP One app is designed for mobile device use on iOS, Android phones and a desktop webapp and will be hosted in CACE. CACE will provide data protection, governance, and monitoring services. The audit logging and monitoring functionality in the application is implemented by the Cloud Migration Effort (CME) team and coordinated with the application development team, as needed. This functionality captures database inserts, selections, deletions, schema changes, error logs, and exception logs. User provisioning, identity management, authentication, and permission management for the application is managed through the CBP Identity, Credential, and Access Management (ICAM) process. The application will utilize Hypertext Transfer Protocol Secure (HTTPS) for secure communications. Only the CME and application development teams have access to the back-end system and data.

Once developed, the application will be authorized via significant change under the C2MP authorization boundary.

2. Subjects and Users[3] 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.

Undocumented individuals either seeking entry under the MPP Program (Part One) to participate in ongoing immigration proceedings, or initial entry into the U.S. (Part Two).

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.

For MPP individuals, NGOs to determine whether they should expedite their passage to the POE for Processing. For undocumented traveler arriving in the U.S. for the first time, CBP Officers to process them in USEC (b)(7)(E) for transfer to Immigration and Customs Enforcement (ICE).

3) Data to be received by CBP

a) What information will CBP collect through the mobile application[4]? ***List all data elements.***

From NGOs:
Login.gov information

From Undocumented Individuals:
Part One: Photo and Alien Registration Number

Part Two: Alien registration number, name, birthdate, place of birth, citizenship, height, weight, hair color, eye color, picture, travel documentation (i.e., passport number, document number), known languages, language preference, bodily marks (i.e, scars, moles, tattoos), social media information, employment status (i.e., employed, employers number), asylum status (i.e., have you applied for asylum previously, have you claimed fear of persecution of any other country before), family status, traveling status (i.e., are you alone, who are you traveling with), marital status, spouse information (i.e., name, birthdate, place of birth, citizenship), in-law information (for each in-law: i.e., name, birthdate, place of birth, citizenship), children information (for each child: i.e., name, birthdate, place of birth, citizenship), intended port of arrival, address information abroad

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

[4] 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.

(i.e., street, city, state, zip code, telephone), USA point of contact (i.e., name, relation, street address, city, state, zip code, telephone number).	
b) How is the information stored? *Please describe below.*	□ Locally on the mobile device. ☒ In a backend CBP IT system. □ With a third party vendor. □ Other. Describe________
No information is stored locally on the user's device. CBP does not store the photo but will store the A-number and biographic data, if provided, in a CBP Amazon Web Services Cloud Service (CACE) database for 365 days. This data will be retrievable by CBP employees in the Office of Information Technology in order to provide CBP leadership with anonymized statistics related to workload and record location ability For example, number of submissions, number that required submitting the A-number and biographic data.	
c) Does the mobile application collect Social Security number (SSN) or other elements of Sensitive Personally Identifiable Information (SPII)[5]? Check all that apply.	□ Social Security number ☒ Alien Number (A-Number) ☒ Passport Number □ Bank Account, Credit Card, or other financial account number □ Other. Describe________
d) List the *specific authority* to collect SSN or these other sensitive PII elements	
The following CBP legal authorities permit the collection of border crossing information: Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638; Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354; Aviation and Transportation Security Act of 2001 (ATSA); Enhanced Border Security and Visa Reform Act of 2002; and Tariff Act of 1930 as amended, 19 U.S.C. 66, 1433, 1459, 1485, 1624, and 2071.	
e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.	
Alien Numbers and/or passport numbers are needed to verify a traveler's identification.	
f) Does the mobile application collect other types of sensitive	☒ Location Information[7] ☒ Photos/Videos ☒ Mobile Device ID

[5] 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.

[7] 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.

information[6]? Check all that apply.	☒ Metadata[8] ☐ Other. Describe________
g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.	
Photos are required to verify identification. Device ID is required for push notifications which will provide status updates. The goal would be to keep the user abreast of the status of information submitted in advance of arrival. The users can disable notifications through their respective devices as opposed to in the application itself.	

4. Notices	
a) Are individuals provided notice[9] at the time of collection by DHS? If yes, please include a copy of the notice(s) with this PTA upon submission.	☒ Yes. Please describe. ☐ No. Please describe.
CBP One App Specific: Notice of the collection of PII will be provided to the user in the Terms and Conditions before entering the application. A copy of this document is provided with the submission of the PTA. NGO Functionality Specific: Additionally, the NGO collect information from undocumented individuals and submits that information to CBP, through CBP One™. NGOs are responsible for notifying each traveler about information collected and submitted to CBP through CBP One™.	

5. Disclosures	
a) Does the mobile application provide "just-in-time"[10] 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. ☒ No. Please describe.
N/A	

[6] 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).

[8] 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.

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

[10] 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. ☒ No. Please describe.

The CBP One App functionality will interact with the following systems to perform pre-verification and validation: (b)(7)(E)

6. Opt-out Features

a) Does the mobile application provide users with independent opt-out features[11] 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. ☒ No. Please describe.

There are no services from which to opt-out. Users can choose to opt-out from notifications via their respective devices.

7. Mobile App-Specific Privacy Policy

a) Does the mobile application have an App-Specific Privacy Policy[12] 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[13] upon submission.	☒ Yes. Please describe. ☐ No. Please describe.

The Privacy Policy is listed in the application's Terms and Conditions. DHS approved a CBP One Mobile App Privacy Policy with the original submission of the CBP One PTA.

8. DHS Carwash process?

[11] 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

[12] 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

[13] 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

a) Has this mobile application been through the DHS Carwash[14] process?	☐ Yes. **Please provide the results of the Carwash with this PTA.** ☒ No. Please describe.
The NGO functionality has not been submitted through the DHS AppVet scan, however OIT will work to submit this as soon as possible.	

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:	**February 10, 2021**
Date submitted to DHS Privacy Office:	Click here to enter a date.
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)	

[14] 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 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:	February 10, 2021
PTA Expiration Date	March 10, 2021

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. Click here to enter text.
PIA:	**New PIA is required. CBP One Mobile Application PIA** If covered by existing PIA, please list: DHS/CBP/PIA-012 – CBP Portal (e3) to ENFORCE/IDENT; DHS/CBP/PIA-067 U.S. Customs and Border Protection Unified Secondary 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; DHS/CBP-013 Seized Assets and Case Tracking System, December 19, 2008, 73 FR 77764; DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601; DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017, 82 FR 43556; DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, October 19, 2016, 81 FR 72080; DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792

	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)

Homeland Security

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application	CBP One™ Mobile Application, I-94 Mobile Functionality		
DHS Component:	Customs and Border Protection (CBP)	Office or Program	Office of Field Operations
Date of last PTA (if applicable):			
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:	Office of Field Operations (OFO)	Title:	CBP Officer/ CBP Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

OIT MOBILE APPLICATION DEVELOPMENT LEAD

Name:	(b)(6), (b)(7)(C)		
Office:	Office of Information and Technology (OIT)	Title:	Supervisory IT Specialist
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

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.*

CBP is submitting this PTA to document the I-94 Mobile functionality embedded into the CBP One™ Mobile Application.

I-94 Mobile

I-94 Mobile is function of CBP One™ and offers the same features as the current CBP I-94 website application (e.g., apply for a provisional I-94 in advance of arrival, search for their most recent I-94, view travel history, and view compliance). The I-94 Mobile function collects the same biographic, travel document and trip information from nonimmigrant noncitizens as the CBP I-94 website application. Nonimmigrant noncitizens who use the CBP One™ mobile application to apply for an I-94 in advance will be able to quickly scan their travel document information, using the Machine-Readable Zone (MRZ) scan capability built into the mobile application, which will read the biographic data from the traveler's document and enter it into the corresponding data fields in the I-94 mobile function of CBP One™. The MRZ capability streamlines the data entry process when users apply for an I-94 in advance of arrival. CBP One ™ users are still required to submit their payment through Pay.gov.

CBP recently incorporated a technical system change into CBP One™ and the I-94 website, allowing some undocumented noncitizens who entered without a foreign passport, such as those processed under the Migrant Protection Protocols (MPP) program, the ability to utilize their Alien-number (A number) to search, retrieve and print their most recent electronic Form I-94. This is used by undocumented noncitizen travelers (to include MPP travelers) as a means to provide proof of their legal admission (or parole) into the United States. Additionally, the "View Travel History" module for both I-94 website and CBP One mobile app returns 10 years of travel history. Further details on this capability will be available in the forthcoming CBP I-94 Web Application PIA Update.

In October 2021, CBP modified the CBP One™ mobile application, traveler functionality to allow undocumented noncitizens, who are a part of Operation Allies Welcome, and who are within the age of 14 to 79 years old, to search by their facial photograph and retrieve their most recent electronic I-94. Undocumented noncitizens will use their electronic I-94 to verify their identity during the resettlement process. Individuals must first create a new or open an existing Login.Gov account in order to access CBP One™. Once a user has access to the traveler functionality in CBP One™, he or she will be able to use the application to retrieve their electronic I-94. The user must first select their mode of travel "air" or "land", and then select "Get My Recent I-94". The user will then select "Search for an I-94", and

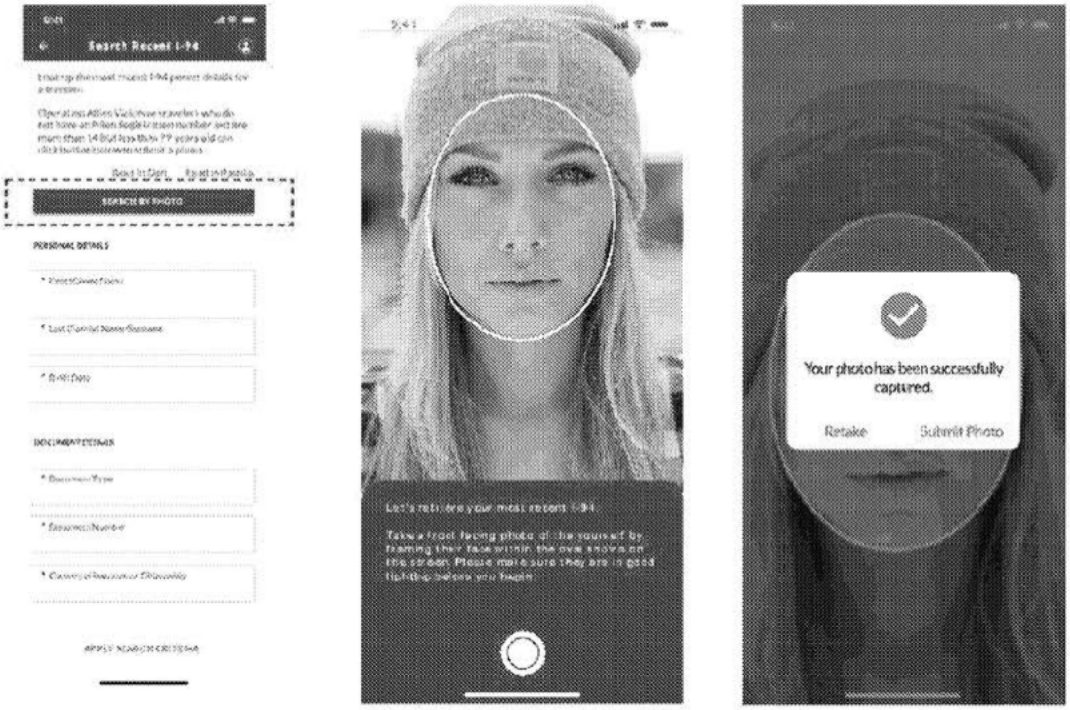
[1] DHS defines DHS Mobile Application (DHS Mobile App) as a native software application that is developed by, on behalf of, or in coordination with DHS for use on a mobile device (e.g., phone or table) by DHS employees and/or the public.

"Search by Photo" and submit a facial photograph of him or herself through the CBP One™ mobile application. CBP One™ uses TVS , a facial matching service, to templatize and match the live facial photograph captured from the undocumented noncitizen through CBP One, against a facial photograph from an existing staged gallery. The staged gallery is populated with images of the refugees from the SaAW database/ATS. ATS retrieves refugees' facial photographs from IDENT , and these facial photographs are sent to the staged refugee gallery in the SaAW database.

If a match is made, CBP One™ will return the following information on the screen: First Name, Last Name, Date of Birth, Alien Identification Number (A-number) (if available), citizenship of the traveler, admission (I-94) record number, most recent date of entry, class of admission, and admit until date. CBP One™ will return a red "X" if no match is found. In the event of a "no match" or if the user declines to be photographed, they can input their biographic information and CBP One™ will attempt to match against the SaAW/ATS databases to retrieve the travelers I-94 information.

As with other CBP One™ uses, no information is stored locally on the device. CBP does not store the photo but will store the A-number and biographic data, if provided, in a CBP Amazon Web Services Cloud Service (CACE) database for 365 days. This data will be retrievable by CBP employees in the CBP Office of Information Technology in order to provide CBP leadership with anonymized statistics related to workload and record location ability. For example, CBP employees will be able to view number of submissions and number of submissions that required submitting the A-number and biographic data.

CBP One – **Traveler: Land Get My Recent I-94 > Take Photo**



Search Recent I-94

Look up the most recent I-94 permit details for a traveler.

Operation Allies Welcome travelers who do not have an Alien Registration number and are more than 14 but less than 79 years old can click button below to submit a photo.

PERSONAL DETAILS

* First (Given) Name

* Last (Family) Name/Surname

* Birth Date

DOCUMENT DETAILS

* Document Type

* Document Number

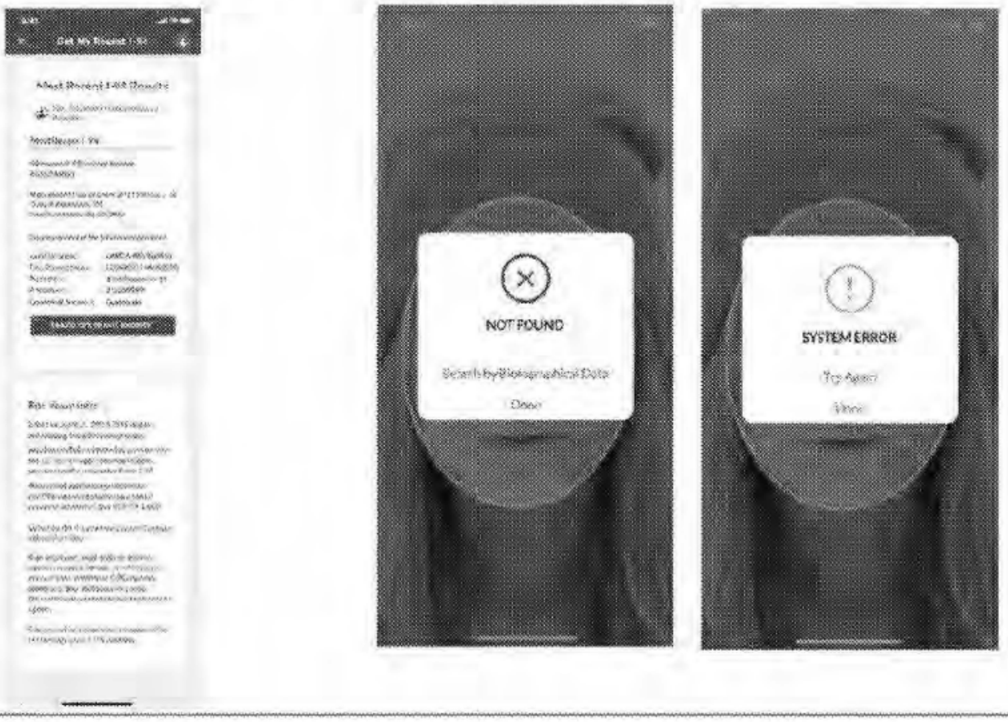
* Country of Issuance or Citizenship

Let's retrieve your most recent I-94.

Take a front facing photo of the yourself by framing their face within the oval shown on the screen. Please make sure they are in good lighting before you begin.

Your photo has been successfully captured.

CBP One – **Traveler: Land > Get My Recent I-94 > Query Results after Photo**



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.
Members of the public will submit information into the CBP One, I-94 Mobile functionality.	
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.

- Members of the public can use I-94 Mobile to: apply for a provisional I-94 in advance of arrival, search for their most recent I-94, view travel history, and view compliance.
- CBP Officers (CBPOs) will use the information members of the public submit through the I-94 Mobile to view an I-94 application when the traveler arrives at a port of entry using Passenger Admissibility systems (i.e. (b)(7)(E)). CBPOs

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

reviewing the I-94 application information will use the information to vet the applicant and issue an I-94 permit. This includes the payment information. CBP uses pay.gov to collect payment information. CBP One does not collect or store the cc #, bank account #,or other financial account information.This replicates the same functionality as if the traveler had submitted their I-94 application using the CBP I-94 website.

- CBP employees/contractors may also use the information travelers submit through the I-94 mobile for analytical reporting (i.e., mobile application usage reports, overstay analysis, etc.)

All PII collected through the I-94 mobile functionality, within the CBP One Mobile App, may not be used for any purpose other than those outlined in the applicable SORNs.

3) Data to be received by CBP

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

I-94 Mobile /Travelers & Co-Travelers Information

CBP collects the same biographic, travel document and trip information from the traveler through CBP One- I-94 Mobile, and the CBP I-94 website application. The biographic, travel document, and trip information data fields are listed below.

Travel and Co-Traveler- Biographic Information

- First Name
- Middle Name
- Last Name
- Date of Birth
- Gender
- Country of Residence
- Country of Citizenship
- SEVIS number (Optional)
- Petition (Optional)

Travel and Co-Traveler- Document Information may include:

- Document Type
- Document Number
- Issue Date
- Issue Country

[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.

- Expiration Date

Traveler and Co-Traveler – Visa Information (Optional)

- Visa Number
- Issue Date
- Issue Country

Traveler and Co-Traveler -Contact Information

- Phone Number
- Email

Traveler and Co-Traveler -Address while in the U.S. Information

- Street
- City
- State
- Zip

Travel and Co-Traveler -Mode of Travel

- Air (New Mode of Travel, incorporated in October 2021)- Only available through CBP One
- Land

In addition, the I-94 Mobile collects biometric information from undocumented noncitizens only through the CBP One mobile application. This change was incorporated into the mobile application in October 2021. Biometric information is not collected through the CBP I-94 website application.

Biometric Information (New Collection)

- Facial Photograph (Selfie)

b) How is the information stored? *Please describe below.*	X Locally on the mobile device. X In a backend CBP IT system. ☐ With a third party vendor. ☐ Other. Describe________

ADIS is the system of record for all I-94 data. All biographic and travel document information collected through the CBP One, I-94 Mobile functionality is sent to ADIS.

In addition, CBP does not store the facial photograph but will store the A-number and biographic data, if provided, in a CBP Amazon Web Services Cloud Service (CACE) database for 365 days. This data will be retrievable by CBP employees in the CBP Office of Information Technology in order to provide CBP leadership with anonymized statistics related to workload and record location ability. For example, CBP employees will be able to view number of submissions and number of submissions that required submitting the A-number and biographic data.

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 **X** Alien Number (A-Number) **X** Passport Number Bank Account, Credit Card, or other financial account number **X** Other. Describe: **Border Crossing Card (BCC), Visa Number, and Biometric Facial Photograph (Selfie)**

d) List the *specific authority* to collect SSN or these other sensitive PII elements

CBP authority to collect information from the traveler via CBP One™ is codified through the Paperwork Reduction Act, 44 U.S.C. § 3501, which supports the automated I-94 process; the OMB Control Number is 1651-0111.

Authorities supporting CBP's collection and use of the I-94 data include: 8 U.S.C. § 1103. Powers and duties of the Secretary, the Under Secretary, and the Attorney General; 50 U.S.C. 401 §§ et seq., The Intelligence Reform and Terrorism Prevention Act of 2004; 8 U.S.C. §§ 1101 et seq., The Immigration and Nationality Act; and 6 U.S.C. §§ 101 et seq., the Homeland Security Act of 2002.

The following legal authorities allow DHS to create a biometric entry and exit program: The 1996 Illegal Immigration Reform and Immigrant Responsibility Act, Pub. L. No.104-208, 110 Stat. 3009-546; 2002 Enhanced Border Security and Visa Entry Reform Act, Pub. L. No. 107-173, 116 Stat. 543, 552; Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, 3817; Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266, 338; Consolidated Appropriations Act of 2016, P.L. 114-113 129 Stat. 2242 (December 17, 2015); and Executive Order 13780, "Protecting the Nation from Foreign Terrorist Entry into the United States."

e) Describe *why* this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

I-94 Mobile- The information collected through I-94 mobile is necessary for CBP to make entry screening and admissibility determinations, to inform any future applicable benefits related to immigration and for law enforcement purposes.

f) Does the mobile application collect other types of sensitive	Location Information[6] **X** Photos/Videos – **I-94 Mobile** Mobile Device ID

[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.

[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.

information[5]? Check all that apply.	Metadata[7] Other. Describe:
g) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.	

I-94 Mobile

- Facial Photograph/Selfie to is required for biometric comparison for undocumented noncitizens considered to be in the OAW population.

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.

The traveler is informed during launch of the CBP One mobile application that this is an official system and that they are accepting the terms and conditions. Additionally, CBP has issued a privacy policy and this embedded into CBP One™. The privacy policy appears as traveler logs into CBP One™, and the traveler must consent to this notice prior to using the mobile application.

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)?	X Yes. Please describe. ☐ No. Please describe.

I-94 Mobile

Upon entry into the app, the traveler will have the option to provide their consent to enable the cell phone camera. *A notification for consent will only appear each time, if the user does not consent to the application the first time to enable the cellphone permission.*

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

[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).

[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.

[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)

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.
I-94 Mobile Undocumented Noncitizens considered to be in the OAW population: The mobile device user must provide permission for the CBP One mobile application to use their mobile device camera, , or they cannot successfully report their mobile exit via the I-94 mobile application.	

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.	X Yes. Please describe. ☐ No. Please describe.
CBP One has an overarching privacy policy that discusses the I-94 mobile functionality. CBP Privacy recently updated the CBP One privacy policy and this is attached to this PTA submission.	

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.

[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

[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.

This PTA submission includes updated DHS AppVet results for the CBP One, I-94 Mobile.	

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:	**October 6, 2021**
Date submitted to DHS Privacy Office:	October 7, 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)

(b)(5)

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
PCTS Workflow Number:	(b)(6)
Date approved by DHS Privacy Office:	May 11, 2022
PTA Expiration Date	May 11, 2025

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. Click here to enter text.
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: • DHS/CBP/PIA-016(a) I-94 Web Application; • DHS/CBP/PIA-068 CBP One Mobile Application; • DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS) If a PIA update is required, please list:
SORN:	**System covered by existing SORN** If covered by existing SORN, please list: • DHS/CBP-016 Nonimmigrant Information System, March 13, 2015, 80 FR 13398 • 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 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)

Homeland Security

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 Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application:	**CBP One™ DHS Persona (Consolidation and Capabilities)**		
DHS Component:	**Customs and Border Protection (CBP)**	Office or Program:	**Planning, Program Analysis and Evaluation (PPAE)**
Launch date:	Click here to enter a date.	Project or program status:	Choose an item.
Date of last PTA (if applicable):	Click here to enter a date.		

MOBILE APP DEVELOPMENT PROGRAM MANAGER/BUSINESS OWNER

Name:	(b)(6), (b)(7)(C)		
Office:	Office of Field Operations (OFO) PPAE	Title:	Program Manager
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

MOBILE APP DEVELOPMENT LEAD/INFORMATION SYSTEM SECURITY OFFICER (ISSO)

Name:	(b)(6), (b)(7)(C)		
Office:	CBP Office of Information and Technology (OIT)	Title:	Supervisory IT Specialist
Phone:	(b)(6), (b)(7)(C)	Email:	(b)(6), (b)(7)(C)

Mobile App Specific-PTA QUESTIONS

1. Purpose of DHS Mobile Application

1. Describe the DHS mobile application[1]. *Please provide a general description of the mobile app and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades that are triggering the update to this PTA. If this is a renewal PTA, please state whether or not there were any changes to the mobile app since the last version.*

Scope: Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is submitting this CBP One™ Mobile Application DHS Persona PTA to consolidate the existing TSA Persona PTA into the CBP One™ DHS Persona PTA. This PTA also combines the purposes and capabilities of the DHS Persona into a single PTA. The consolidated DHS Persona provides the following three capabilities: (1) Retrieve Traveler Information; (2) Retrieve Refugee Information; and (3) Retrieve Appointment Information. This PTA supersedes previously adjudicated PTAs cited below.

Previous Related PTAs

CBP previously submitted separate PTAs to account for the creation of the TSA Persona (see "PTA, CBP - CBP One™ Mobile Application – TSA Functionality," dated February 24, 2021) and then the DHS Persona (see "PTA, CBP – CBP One™ Mobile Application, New PTA – Department of Homeland Security Persona & Use Case for Federal Agencies," dated November 4, 2021). A third related PTA accounts for the CBP One™ use case in which TSA employees process undocumented Afghan refugees subject to security screening prior to boarding domestic flights. (see "PTA, CBP - CBP One™ Mobile Application, TSA Use Case - Update PTA DHS Persona & Afghan Refugees," dated November 4, 2021).

DHS Persona

In November 2021, CBP created the DHS Persona within CBP One™ to enable appropriately credentialed DHS (including CBP and the U.S. Citizenship and Immigration Service (USCIS)) and Department of Defense (DoD) users using government-issued devices to collect information from undocumented noncitizens and verify those individuals' identities at security checkpoints to permit further travel within the United States and for purposes of resettlement. Earlier in 2021, CBP created a TSA Persona in CBP One™ to permit correspondingly credentialed TSA employees to collect similar types of information for the purpose of identity verification for certain undocumented noncitizens who required security screening prior to entering airport sterile areas and boarding domestic flights. CBP created the DHS Persona and TSA Persona for specific use cases related to the processing of undocumented noncitizens during Migrant Protection Protocol (MPP), Operation Allies Welcome (OAW) and ongoing processing of undocumented noncitizens who entered on the southwest border. CBP is consolidating the existing personae (i.e., TSA Persona and DHS Persona) into a single DHS

[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. For more information, please see DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

Persona with three capabilities: (1) Retrieve Traveler Information; (2) Retrieve Refugee Information; and (3) Retrieve Appointment Information.

Access to the DHS Persona and the Persona's Capabilities.

CBP placed several controls on access to the DHS Persona. Only authorized DHS (CBP and TSA) users, with Login.gov accounts created using their official email addresses (i.e., with the DHS domain name in the email address: @cbp.dhs.gov or @tsa.dhs.gov), using the CBP One™ application on government-issued devices, will have access to the DHS Persona. DHS users will not have access to any other CBP One™ modules or capabilities while accessing the DHS Persona. Other CBP One™ users, for example, members of the public who use CBP One™, will not see or have access to the DHS Persona.

DHS Persona Capabilities

1. RETRIEVE TRAVELER INFORMATION CAPABILITY

TSA employees use the DHS Persona Retrieve Traveler Information capability to perform the necessary security screening by verifying the identity of undocumented noncitizens. Undocumented noncitizens are individuals who, otherwise, would not be permitted to travel within the United States due to the lack of travel documentation or would be subject to a lengthy identity verification process. Previously, CBP limited use of this capability to Afghan refugees and MPP enrollees use cases. Now, CBP will use the Retrieve Traveler Information capability to the broader population of undocumented noncitizens beyond the initial two use cases.

Using the Retrieve Traveler Information capability, authorized TSA users at security checkpoints (i.e., at the entry to airport sterile areas and prior to boarding domestic flights) use CBP One™ to collect information from a traveler with the traveler's consent. The TSA user collects the information either by taking the traveler's live photo with the government-issued mobile device or by collecting basic biographic information from the traveler. The Retrieve Traveler Information capability submits the collected information to match images, i.e., biometrically confirm the photos, and/or retrieve other limited biographic information about the individual from existing CBP galleries pre-staged for this purpose from CBP's Automated Targeting System (ATS) Seizure and Arrest Workflow (b)(7)(E) and I-94 databases. Matching the information collected from the traveler with the information retrieved from the existing databases provides the required identity verification for the traveler. The pictures taken by TSA employees of undocumented noncitizens are matched against the pre-staged gallery for identity verification purposes only.

The Traveler Information Retrieval Process

There are up to three ways for the DHS Persona user to retrieve the traveler's information involving the collection of a photo or biographic data and/or A-Number, as described further.

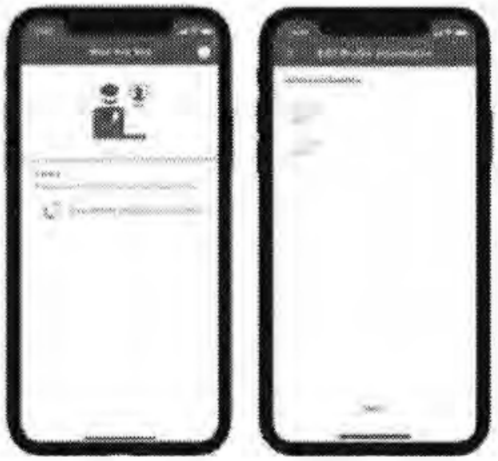
- **By Means of a Photo**

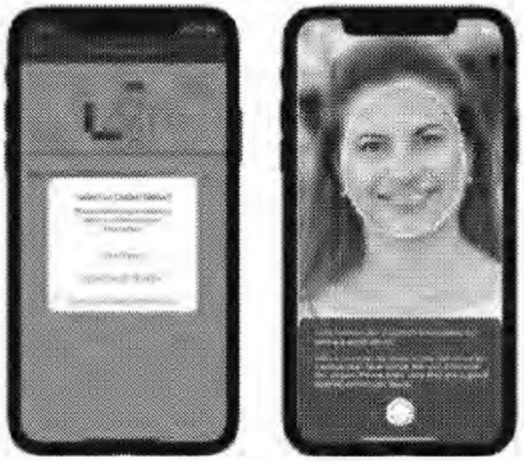
DHS Persona users can take a live photograph of the undocumented noncitizen individual with the government-issued device and enter the photo into the CBP One application. Using CBP's Traveler Verification Service (TVS) facial comparison technology, the application attempts to match the photo in a gallery of photos pre-staged from different CBP databases, depending on the use case.

CBP One™ Retrieve Traveler Information Screenshots

1. Who Are You
Tap on "Department of Homeland Security" to begin. First time users will be prompted to create a profile.

2a. TSA at Security Checkpoints: Utilize "Retrieve Traveler Information"
Select one of the options provided. "Take a Photo", "Search by A-Number" or "Search by Biographical Data".





- CBP One™ matches against pre-staged images populated from the CBP ATS (b)(7)(E) database

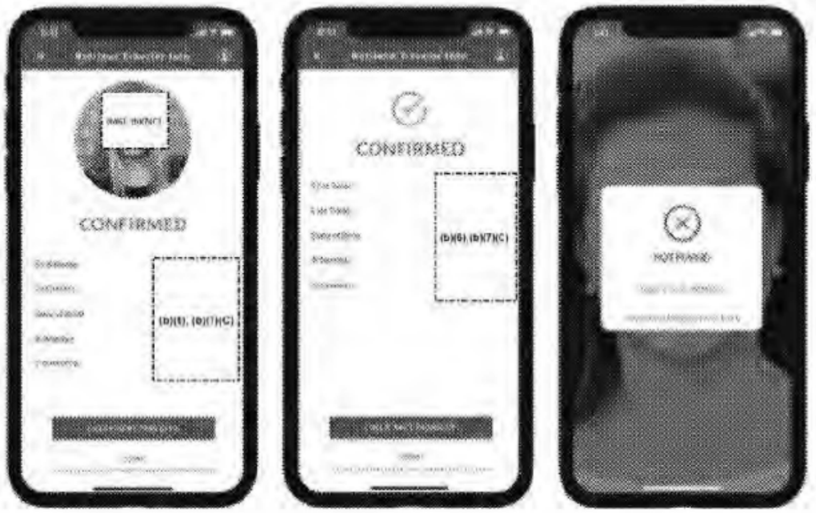
If a match is made, CBP One™ will use the biographic information associated with the image to locate the individual's information in the I-94 database. CBP One™ will send a green check mark and return the following information:

- First Name
- Last Name
- Date of Birth
- Alien Identification Number (A-number) (if available)
- Citizenship

CBP One™ Retrieve Traveler Information Match Results Screenshots

3a. TSA at Security Checkpoints

Confirmed" will retrieve the traveler's first/last name, DOB, A-Number, citizenship, and photo (if they have one).



- **By Biographic Data and/or A-Number**

If no match is found, CBP One™ returns a red "X" "Not Found." In the event of a red X result or if the traveler declines to be photographed, the TSA user can search by the traveler's biographic information or A-Number with the traveler's consent. CBP One™ will attempt to match the biographic data or A-Number entered into the mobile application against the ATS (b)(7)(E) database.

Like the photograph submission, described above, the biographic information- or A-Number-based search will return either a green check mark or red "X" to the TSA user through CBP One™. If the TSA user gets a red "X," the user can contact the National Transportation Vetting Center to determine if the traveler should not be permitted to continue through the screening process.

Data Storage and Retention

As with other CBP One™ uses, no information is stored locally on the user's device. CBP does not store the photo but will store the A-number and biographic data, if provided, in a CBP Amazon Web Services Cloud Service (CACE) database for 365 days. This data will be retrievable by CBP employees in the Office of Information Technology to provide CBP leadership with anonymized statistics related to workload and record location ability. For example, number of submissions, number that required submitting the A-number and biographic data. TSA does not store any of the information. TSA uses the data only to verify identity during the in-person encounter.

2. RETRIEVE REFUGEE INFORMATION

In the past, USCIS and DoD assisted with the Operation Allies Welcome (OAW) resettlement efforts for Afghan refugees. DoD personnel provided essential support at secure military bases, where Afghan refugees can safely complete the necessary steps for resettlement in the United States. Authorized DHS and DoD personnel used the DHS Persona to verify the identity of refugees during various stages of OAW resettlement processing to include intake and resettlement.

DHS and DoD completed their use of this DHS Persona capability in support of processing OAW Afghan refugees. CBP removed access to the DHS Persona for USCIS and DoD users as a result. However, the DHS Persona retains this information retrieval capability in reserve for use in meeting identification needs for future refugee identity verification use cases. This PTA includes the discussion below about the OAW information retrieval process as an example of how future refugee information may be collected and handled. CBP One™ will consult with the CBP Privacy Office prior to operationalizing the capability for future refugee use cases to complete any necessary documentation updates.

The OAW Information Retrieval Process

The Retrieve OAW Information capability provided identity verification only using photograph matching. The DHS Persona user took a photograph of a refugee on his or her government-issued device. CBP One™ used the TVS facial comparison technology to match the refugee's photograph with a photograph in an existing staged gallery to verify the refugee's identity in CBP systems. The staged gallery was populated with all the images from the ATS (b)(7)(E) database. ATS retrieved refugees' facial photographs from IDENT and sent these facial photographs to the pre-staged refugee gallery in the (b)(7)(E) database. In addition, the (b)(7)(E) database pulled I-94 biographic information from the I-94 database and transmitted this information back to the CBP One™ mobile application.

If a match was made, CBP One™ returned the following information to the DHS or DOD users:

- First Name
- Last Name
- Date of Birth
- Alien Identification Number (A-number) (if available)
- Hummingbird Case Number (H-Number) (if available)
- Admission (I-94) Record Number
- Most Recent Date of Entry
- Class of Admission
- Admit Until Date
- Facial photograph of the traveler (if available).

As with other DHS Persona uses, CBP One™ returned a red "X" if no match was found. If the Refugee was not found in the CBP One™ application, the DHS or DoD component users had to use other means of verifying identity such as a printed I-94 or other form of identification issued at safe haven or resettlement areas. DHS and DoD component users did not have the option to search by the undocumented noncitizens biographic or Alien number through the CBP One™ application.

Data Storage and Retention

As with other CBP One™ uses, no information was stored locally on the device. DHS and DoD components did not store the facial photograph.

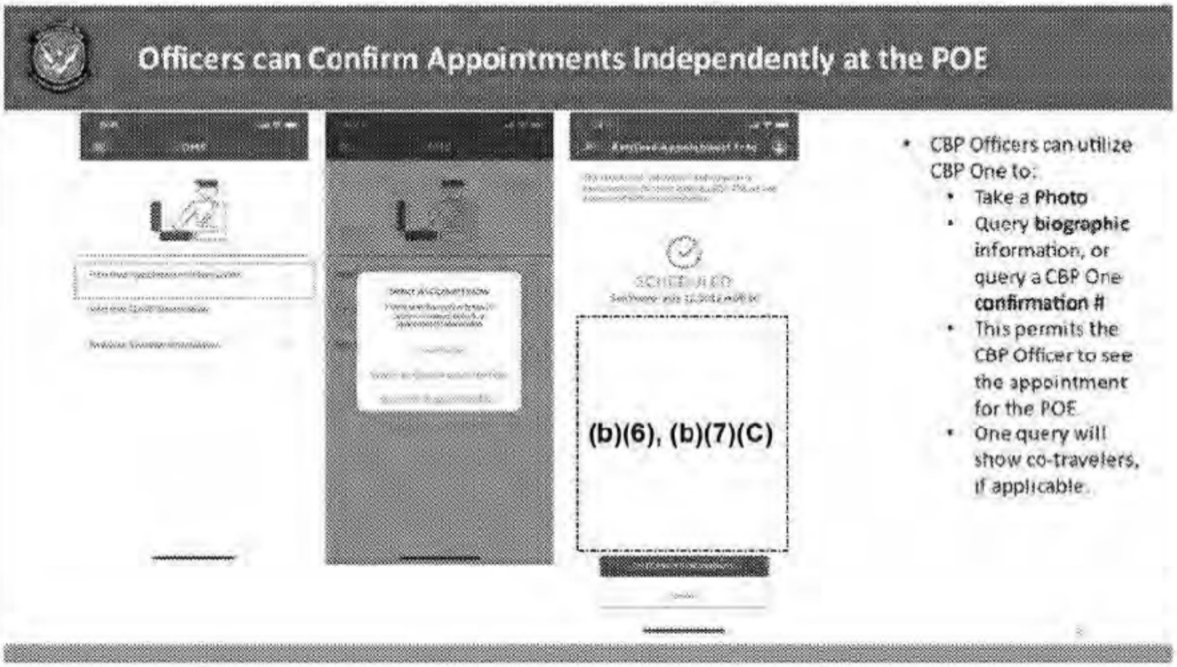
3. RETRIEVE APPOINTMENT INFORMATION

CBP Officers use this DHS Persona capability to validate information from undocumented noncitizens who present at a Southwest Border POE claiming to have a CBP One™ appointment.

The Appointment Information Retrieval Process

CBP Officers can enter and search the CBP One™ CBP Amazon Web Service (AWS) Cloud Environment (CACE) database by an individual's appointment confirmation number or biographic data or the Officer can take and submit a photo of the individual. CBP One™ returns the individual's' previously submitted photo, biographic, and appointment information for the individual and all other individuals in the same submission.

CBP One™ Retrieve Appointment Information Screenshots



Officers can Confirm Appointments Independently at the POE

- CBP Officers can utilize CBP One to:
  - Take a **Photo**
  - Query **biographic** information, or query a CBP One **confirmation #**
  - This permits the CBP Officer to see the appointment for the POE
  - One query will show co-travelers, if applicable.

Data Storage and Retention

As with other CBP One™ uses, no information is stored locally on the device.

Retrieve Traveler Information Capability

CBP will store the A-number and biographic data, if provided, in a CBP Amazon Web Services Cloud Service (CACE) database for 365 days.

Retrieve Refugee Information

CBP stores no information for this capability.

Retrieve Appointment Information

CBP will store an individual's appointment confirmation number or biographic data in the CBP One™ CACE database for 365 days.

2. Subjects and Users[2] of the Mobile Application Information

a. Who will SUBMIT information into this mobile application? *Please describe below, including what Components if it involves DHS personnel.*	☒ Members of the public ☒ DHS personnel ☒ Other federal employees

Retrieve Traveler Information
TSA employees submit information collected with consent from undocumented noncitizen travelers.

Retrieve Refugee Information
DHS and DoD employees will submit information collected with consent from undocumented noncitizens into the CBP One™ mobile application using the DHS Persona.

Retrieve Appointment Information
CBP employees will submit information collected with consent from undocumented noncitizens who present at the Southwest Border limit line.

b. Who will USE the information submitted to DHS from this mobile application? *Please describe below, including what Components if it involves DHS personnel.*	☐ Members of the public ☒ DHS personnel ☒ Other federal employees

Traveler Information
TSA employees will use the information submitted and retrieved through CBP One™ to perform identity verification of undocumented noncitizens at the entry to airport sterile areas and prior to boarding domestic flights.

Refugee Information
DHS and DoD employees will use the information submitted and retrieved through CBP One™ to verify the identity of undocumented refugees during various stages of OAW resettlement processing to include intake, employment, and resettlement.

Appointment Information
CBP employees will use the information submitted and retrieved through CBP One™ to confirm appointments made by undocumented noncitizens through CBP One™ who present at the Southwest Border limit line.

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

3) Data to be collected

a) What information will be submitted through the mobile application? *Please list all data elements.*

Traveler Information
Facial photograph and/or biographic information and/or alien registration number

Refugee Information
Facial photograph

Appointment Information
Facial photograph and/or biographic information and/or appointment confirmation number

b) Does the mobile application collect Sensitive Personally Identifiable Information (SPII)?[3] 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 ☐ DHS Electronic Data Interchange Personal Identifier (EDIPI) ☐ Social Media Handle/ID ☐ Known Traveler Number/Other Traveler ID Number ☐ Driver's License Number ☒ Biometrics (e.g., fingerprints, facial images/photographs) ☐ Other. Please list:

c) List the *specific authority* to collect SSN or these other SPII elements. *Note*: even if the program is properly authorized to collect SSNs, you are required to use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking/truncating the SSN, or blocking the display of SSNs within the mobile application.[4]

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat. 3638; Immigration and Nationality Act, as codified at 8 U.S.C. 1185 and 1354; Aviation and Transportation

[3] DHS defines Sensitive Personally Identifiable Information (SPII) as 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.

[4] Please see DHS Instruction Number: 047-01-009 (Social Security Number Collection and Use Reduction).

Security Act of 2001 (ATSA); Enhanced Border Security and Visa Reform Act of 2002; and Tariff Act of 1930 as amended, 19 U.S.C. 66, 1433, 1459, 1485, 1624, and 2071.

d) Describe *why* this collection of SPII is necessary and the minimum amount of information required to accomplish the purpose of the program.

Photographs and/or A-numbers are required to verify identification.

e) Does the mobile application collect other types of sensitive content information?[5] Check all that apply.	☐ Location Information[6] ☒ Photos/Videos[7] ☐ Mobile Device ID ☐ Metadata[8] ☐ Other. Please list:

f) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.

Undocumented noncitizens may not have a valid travel document to present. The CBP One™ Mobile Application collects the facial photograph from undocumented noncitizens to verify their identity prior to domestic travel or to confirm an undocumented noncitizen's appointment information.

g) How and where is the information stored? *Please describe below.*	☐ Locally on the mobile device ☒ In a back-end DHS system ________________ ☐ With a third-party vendor ☐ Other. Describe________

h) How long is information stored or retained? If the data is stored in multiple places, please provide the information for all locations. *Please describe below and indicate retention schedules if applicable.*

Traveler Information

As with other CBP One™ uses, no information is stored locally on the user's device. CBP does not store the photo but will store the A-number and biographic data, if provided, in a CBP CACE database for 365 days.

[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] Photos/videos meaning the mobile app access the device's camera or photo library.

[8] 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.

Refugee Information
As with other CBP One™ uses, DHS stored no information is locally on the device. DHS will not store the facial photograph.

Appointment Information
As with other CBP One™ uses, no information is stored locally on the device. CBP will not store the facial photograph. CBP will store an individual's appointment confirmation number or biographic data in the CBP One™ CACE database for 365 days.

i) How do you ensure that information is disposed of or deleted in accordance with the retention schedule?

CBP One™ stores no information.

j) Does the project, program, or system retrieve information by personal identifier?	☒ Yes. Please list personal identifiers below. ☐ No.

Facial photograph, and/or name, and/or A-Number

4. Notices

a) Are individuals provided a Privacy Act Statement, Privacy Notice, or some, other type of notice[9] at the time of collection by DHS? If yes, please include a copy of the notice(s) with this PTA upon submission.	☒ Yes. ☐ No.

CBP One™ App Specific: Notice of the collection of PII is currently provided to the user in the Terms and Conditions before entering the application. CBP is working to update the Terms and Conditions to persona-specific Privacy Act Statements.

Department of Homeland Security (DHS) Persona Specific: DHS CBP One™ users collect information from undocumented noncitizens and submit that information to CBP, through CBP One™. DHS component users are responsible for notifying each traveler about information collected and submitted to CBP through the CBP One™ mobile application.

5. Disclosures

a) Does the mobile application provide "just-in-time"[10] disclosures to obtain user's affirmative express consent before a DHS mobile app accesses sensitive content or other tools and applications on the mobile	☐ Yes. Please describe. ☒ No. Not applicable for this persona.

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

[10] 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).

device for the first time (e.g., location services)?	
b) Does the mobile application provide any information to other DHS Components or systems?	☐ Yes. Please describe. ☒ No.
c) Does the mobile application provide any information to third parties (any organization outside of DHS)?	☐ Yes. Please describe. ☒ No.

6. Opt-out Features	
a) Does the mobile application provide users with independent opt-out features[11] 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. ☒ No.
b) Before allowing a user to submit information to DHS, does the mobile application provide a "review before sending" function that allows users to correct or opt-out of sending their information to the Department?	☐ Yes. Please describe. ☒ No.

7. Mobile App-Specific Privacy Policy	
a) Does the mobile application have an App-Specific Privacy Policy[12] 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 upon submission.	☒ Yes. Please describe. ☐ No.
The Privacy Policy is listed in the application's Terms and Conditions. DHS approved a CBP One™ Mobile App Privacy Policy with the original submission of the CBP One™ PTA.	

[11] 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.

[12] All DHS Mobile apps are required to have a Privacy Policy that is easily accessible to users through the commercial app store before installation as well as within the app, itself, after installation. This Privacy Policy should be app-specific and cannot merely reference the DHS website Privacy Policy. For more information, please see DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

8. DHS AppVet process?	
a) Has this mobile application been through the DHS AppVet[13] process?	☒ Yes. **Please provide the results of the AppVet with this PTA.** ☐ No.

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:	Click here to enter a date.
Date submitted to DHS Privacy Office:	July 12, 2023
Concurrence from other Components involved (if applicable):	Click here to enter text.

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 AppVet is the service sponsored by DHS Office of the Chief Technology Officer (OCTO) 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 AppVet also performs iterative scans and tests on source code in order to provide insight on code security, quality, and accessibility. DHS AppVet replaced the DHS Carwash. This is a requirement of DHS Directive 047-01-003: Privacy Policy for DHS Mobile Applications, available at https://www.dhs.gov/publication/privacy-policy-dhs-mobile-applications.

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
PCTS Workflow Number:	**0014879**
Date approved by DHS Privacy Office:	August 7, 2023
PTA Expiration Date	August 7, 2024
DHS Privacy Office Approver (if applicable):	Click here to enter text.

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/Privacy Notice required. ☒ Privacy Policy required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. □ Specialized training required. □ Other. Click here to enter text.
e(3)/ Privacy Notice	
Privacy Policy	**Current Privacy Policy sufficient**
PIA:	**PIA Appendix update required** If covered by existing PIA, please list: DHS/CBP/PIA-068 CBP One Mobile Application **[appendix update required]**; DHS/CBP/PIA-056 Traveler Verification Service **[appendix update required]**
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; DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601

DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*

(b)(5)

Homeland Security

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 http://dhsconnect.dhs.gov/org/offices/priv/Pages/Privacy-Compliance.aspx 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:	**U.S. Customs and Border Protection (CBP), Travel Documents and Encounter Data (TDED) data share with U.S. Citizenship and Immigration Services (USCIS) Central Index System 2 (CIS2)**		
Component or Office:	Customs and Border Protection (CBP)	**Office or Program:**	Office of Information and Technology (OIT), Passenger Systems Program Directorate (PSPD)
FISMA Name (if applicable):	**TECS Cloud Travel Documents and Encounter Data (TDED)**	**FISMA Number (if applicable):**	(b)(7)(E)
Type of Project or Program:	Choose an item.	**Project or program status:**	**Development**
Date first developed:	**September 20, 2022**	**Pilot launch date:**	**N/A**
Date of last PTA update	**December 14, 2022**	**Pilot end date:**	**N/A**
ATO Status (if applicable):[1]	**Complete**	**Expected ATO/ATP/OA date (if applicable):**	**September 23, 2022**

PROJECT, PROGRAM, OR SYSTEM MANAGER

Name:	(b)(6), (b)(7)(C)		
Office:	**CBP OIT PSPD**	**Title:**	Division Director
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)

[1] The DHS OCIO has implemented a streamlined approach to authorizing an Authority to Operate (ATO), allowing for rapid deployment of new IT systems and initiate using the latest technologies as quickly as possible. This approach is used for selected information systems that meet the required eligibility criteria in order to be operational and connect to the network. For more information, see (b)(7)(E)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Updated PTA

CBP is submitting this updated PTA to document a new connection between CBP TECS Cloud Travel Documents and Encounters Data (TDED) and the U.S. Citizenship and Immigration Services (USCIS) Electronic Immigration System (USCIS ELIS) in support of the cessation of Title 42.

Background

With the cessation of Title 42, the Office of Field Operations (OFO) is promoting the use of the CBP One by undocumented individuals to submit advanced travel information and schedule their arrival at participating ports of entry (POE). Once the arrival is scheduled, the undocumented individual will arrive to the POE on the prescribed date and time selected within CBP One. During the secondary inspection, CBPOs process the undocumented individuals, and in certain cases, if the individual is eligible, the individual will be issued a parole for two years and released.[2]

CBP plans to share the travel encounter information for these paroled individuals with USCIS.

TDED-USCIS ELIS Data Share

Once the CBPO grants parole and documents the admit until date (AUD) in Unified Secondary (USEC), USEC sends the biographic encounter information, including the CBP One Confirmation to ADIS via the I-94 service. TDED will then connect to ADIS to retrieve the biographic encounter information, including the CBP One confirmation number, from ADIS to populate into TECS TDED. In turn, TDED sends this information to USCIS ELIS. The CBP One Number is the trigger to share this information with USCIS ELIS.

USCIS has discretion to grant these foreign nationals employment authorization. Applicants are not entitled to employment authorization. USCIS determines whether to grant discretionary employment authorization on a case-by-case basis, taking into account all factors and considering the totality of the circumstances of each individual case. Upon USCIS ELIS' receipt of the data, USCIS stores the encounter data in support of the applicant's forthcoming Employment Authorization Document (EAD) application. In a separate process, the undocumented individual is required to submit a Form I-765, Application for Employment Authorization, if they seek to work during their parole period. If USCIS approves the Form I-765, it will be approved concurrent with the parole period (2 years).

As part of the existing connection, TDED will also continue to share data with USCIS Central Index System 2 (CIS2), as described in existing PTAs.

[2] Certain foreign nationals may be paroled into the United States under INA 212(d)(5) for urgent humanitarian reasons or significant public benefit.

2. From whom does the Project, Program, or System collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This project does not collect, collect, maintain, use, or disseminate any personally identifiable information[3] ☒ Members of the public ☐ U.S. Persons (U.S citizens or lawful permanent residents) ☒ Non-U.S. Persons ☐ DHS Employees/Contractors (list Components): *Click here to enter text.* ☐ Other federal employees or contractors (list agencies): *Click here to enter text.*
2(a) Is information meant to be collected from or about sensitive/protected populations?	☐ No ☒ 8 USC § 1367 protected individuals (e.g., T, U, VAWA)[4] ☒ Refugees/Asylees ☐ Other. Please list: *Click here to enter text.*

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

The following is data pulled from TECS/TDED and sent to USCIS ELIS and CIS 2 when a border crossing is generated for the non-citizen population:

- First Name
- Last Name
- Date of Birth (DOB)
- Gender
- Country of Birth

[3] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

[4] This involves the following types of individuals: T nonimmigrant status (Victims of Human Trafficking), U nonimmigrant status (Victims of Criminal Activity), or Violence Against Women Act (VAWA). For more information about 1367 populations, please see: DHS Management Directive 002-02, Implementation of Section 1367 Information Provisions, *available at*
(b)(7)(E)

- Country of Citizenship
- Class of Admission
- I-94 Number
- Fingerprint Identification Number (FIN#)
- Document Number (Passport, Visas)
- Document Issue Country
- Arrival Date & Time
- Alien Number
- Identity Encounter ID
- Encounter Date
- Encounter time
- Document Code
- Citizenship Issue Country
- Visa class entry Code
- Receipt Number
- Vetting Approval Indicator (denotating Approved or Denied). All changes in status will be sent for recurring vetting
- Vetting Approval Date (from ATIS)
- Unique application #
- Marital status (from CBP One)
- CBP One confirmation number
- US Address
- Arrival Port of Entry
- Admit Until Date

3(a) Does this Project, Program, or System collect, maintain, use, or disseminate Social Security numbers (SSN) or other types of stand-alone sensitive information?[5] If applicable, check all that apply.

☐ Social Security number

☒ Alien Number (A-Number)

☐ Tax Identification Number

☒ Visa Number

☒ Passport Number

☐ Social Media Handle/ID

☐ Driver's License/State ID Number

☒ Biometric identifiers *(e.g., FIN, EID)*

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

[5] Sensitive PII (or sensitive information) is PII that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. More information can be found in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[6] If related to IDENT/HART and applicable, please complete all Data Access Request Analysis (DARA) requirements. This form provides privacy analysis for DHS` IDENT, soon to be HART. The form replaces a PTA where IDENT is a service provider for component records. PRIV uses this form to better understand how data is currently shared, will be shared and how data protection within IDENT will be accomplished. IDENT is a biometrics service provider and any component or agency submitting data to IDENT is a data provider.

□ Bank Account, Credit Card, or other financial account number □ Driver's License/State ID Number	□ Other. *Please list: Click here to enter text.*
3(b) Please provide the specific legal basis for the collection of SSN:	N/A

3(c) If the SSN is needed to carry out the functions and/or fulfill requirements of the Project, System, or Program, please explain why it is necessary and how it will be used.

N/A

3(d) If the Project, Program, or System requires the use of SSN, what actions are being taken to abide by Privacy Policy Instruction 047-01-010, *SSN Collection and Use Reduction*,[7] which requires the use of privacy-enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN? Note: *even if you are properly authorized to collect SSNs, you are required to use an alternate unique identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as masking, truncating, or encrypting the SSN, or blocking the display of SSNs in hard copy or digital formats.*

N/A

4. How does the Project, Program, or System retrieve information?	☒ By a unique identifier.[8] Please list all unique identifiers used: CBP One Confirmation Number □ By a non-unique identifier or other means. Please describe: *Click here to enter text.*

5. What is the records retention schedule(s) for the information collected for each category type (include the records schedule number)? *If no schedule has been approved, please provide proposed schedule or plans to determine it.*	*Travel Documents and Encounter Data (TDED) records are not currently covered under any schedule. The Business Office will work with CBP RIM to develop a NARA-Approved Records Schedule. Until a schedule has been approved, these records will be held indefinitely and will not be deleted/destroyed.*

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

[8] Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Note: If no records schedule is in place or are unsure of the applicable records schedule, please reach out to the appropriate Records Management Office.[9]	*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)*
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?[10]	□ No. ☒ Yes. If yes, please list: • CBP TECS/Arrival and Departure Information System (ADIS) • USCIS Central Index System 2 (CIS2) • USCIS ELIS
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***	N/A

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

[10] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in IACS.

applicable, please provide agreement as an attachment.	Please describe applicable information sharing governance in place: **Sharing is governed under the One DHS Memo.**
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: **TDED maintains audit information for what data is sent to USCIS and when the data is sent. Data is sent via encrypted SFTP to prevent external access to information.** ☐ 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[11] ☐ Live PII data for testing ☒ No

[11] The autonomous or semi-autonomous examination of Personally Identifiable Information using sophisticated techniques and tools to draw conclusions. Advanced Analytics could include human-developed or machine-developed algorithms and encompasses, but is not limited to, the following: data mining, pattern and trend analysis, complex event processing, machine learning or deep learning, artificial intelligence, predictive analytics, big data analytics.

11. Does this Project, Program, or System use data to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly indicative of terrorist or criminal activity on the part of any individual(s) (i.e., data mining)?[12] This does not include subject-based searches.	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*
11(a) Is information used for research, statistical, or other similar purposes? If so, how will the information be de-identified, aggregated, or otherwise privacy-protected?	☒ No. ☐ Yes. If yes, please elaborate: *Click here to enter text.*

12. Does the planned effort include any interaction or intervention with human subjects[13] via pilot studies, exercises, focus groups, surveys, equipment or technology, observation of public behavior, review of data sets, etc. for research purposes	☒ No. ☐ Yes. If yes, please reach out to the DHS Compliance Assurance Program Office (CAPO) for independent review and approval of this effort.[14]

13. Does the Project, Program, or System provide role-based or additional privacy training for personnel who have access, in addition to annual privacy training required of all DHS personnel?	☐ No. ☒ Yes. If yes, please list: TDED routinely provide system-related training.

[12] Is this a program involving pattern-based queries, searches, or other analyses of one or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

(ii) the security of a Government computer system.

[13] Human subject means a living individual about whom an investigator conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

[14] For more information about CAPO and their points of contact, please see: https://www.dhs.gov/publication/compliance-assurance-program-office or https://collaborate.st.dhs.gov/orgs/STCSSites/SitePages/Home.aspx?orgid=36. For more information about the protection of human subjects, please see DHS Directive 026-04: https://www.dhs.gov/sites/default/files/publications/mgmt/general-science-and-innovation/mgmt-dir_026-04-protection-of-human-subjects_revision-01.pdf.

14. Is there a FIPS 199 determination?[15]	□ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: □ Low □ Moderate ☒ High □ Undefined Integrity: □ Low □ Moderate ☒ High □ Undefined Availability: □ Low □ Moderate ☒ High □ Undefined

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:	**December 15, 2022**
Concurrence from other Component Reviewers involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	December 21, 2022

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)

[15] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

(b)(5)

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6)
DHS Privacy Office Approver (if applicable):	(b)(6)
Workflow Number:	Click here to enter text.
Date approved by DHS Privacy Office:	December 22, 2022
PTA Expiration Date	December 22, 2023

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-021 TECS System: Platform; Advance Collection of Information from Certain Undocumented Individuals PIA **[forthcoming]**
SORN:	**System covered by existing SORN** DHS/CBP-007 Border Crossing Information (BCI), December 13, 2016, 81 FR 89957; DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above, and any further action(s) that must be taken by Component.

(b)(5)

(b)(5)