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

PRIVACY THRESHOLD ANALYSIS (PTA)

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

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

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

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

PIA@hq.dhs.gov

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

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

Privacy Threshold Analysis (PTA)

Specialized Template for Mobile Applications

Summary Information

Name of Mobile Application:	**Mobile Fortify Mobile Application for ICE Enforcement and Removal Operations**		
DHS Component:	**Customs and Border Protection (CBP)**	Office or Program:	**OFO**
Launch date:	**March 25, 2025**	Project or program status:	**Development**
Date of last PTA (if applicable):	N/A		

MOBILE APP DEVELOPMENT PROGRAM MANAGER/BUSINESS OWNER

Name:	(b)(6) (b)(7)(C)		
Office:	CBP TASPD	Title:	
Phone:		Email:	(b)(6) (b)(7)(C)

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

Name:	(b)(6) (b)(7)(C)		
Office:	CBP/OIT	Title:	ISSO
Phone:		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.*

CBP and ICE Privacy are jointly submitting this new mobile app PTA for the ICE Mobile Fortify Mobile App (Mobile Fortify app), a mobile application developed by CBP and made accessible to ICE agents and officers operating in the field. ICE agents and officers will use the Mobile Fortify app to verify (b)(7)(E) identity through facial recognition or contactless fingerprint matching during ICE enforcement operations. (b)(7)(E)
(b)(7)(E)

Background

The Mobile Fortify app will be available for download to ICE issued handheld devices (cell phones or tablets). Users will be authenticated using Airwatch and their PIV credentials on their ICE issued handheld device running Android or iOS.

The Mobile Fortify app is one facet of a Fortify the Border effort. CBP is supporting ICE, as a technical service provider, to assist the DHS mission and carry out the requirements in the January 20, 2025, President Trump signed Executive Order, "Protecting the American People Against Invasion." The Executive Order seeks to faithfully execute immigration laws against all inadmissible and removable aliens, particularly those aliens who threaten the safety or security of the American people. (b)(7)(E)

(b)(7)(E)

(b)(7)(E) The Mobile Fortify App allows ICE agents and officers to use contactless fingerprints (b)(7)(E) and photographs during an encounter for identity verification purposes (b)(7)(E)
(b)(7)(E)
(b)(7)(E) This PTA only covers the Mobile Fortify app portion of the effort. CBP and ICE (b)(7)(E)

(b)(7)(E)

[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.
[2] Contactless fingerprints is a new feature added to existing ATS mobile apps and allows the mobile user to collect fingerprints from a subject just by using the camera embedded in the mobile device. CBP procured this technology from a vendor and has integrated it into the ATS mobile applications.

Process

To conduct identity verification of individuals encountered during an ICE operation (b)(7)(E) (b)(7)(E) ICE agents will use the Mobile Fortify app for biographic and biometric checks. When ICE agents or officers encounter an individual or associates of that individual, they will use the Mobile Fortify app installed on their government-issued device to take a photograph. The photograph is then sent by the application to CBP's Traveler Verification Service, in ATS, (b)(7)(E) (b)(7)(E) as well as the Seizure and Apprehension Workflow that contains the biometric gallery of individuals for whom CBP maintains derogatory information. If no match is made, or a photograph cannot be captured, the ICE agent or officer may then use the Mobile Fortify application to collect contactless fingerprints. Contactless fingerprint captures are then sent via the application to DHS Office of Biometric Identity Management (OBIM) to search against the Automated Biometric Identification System (IDENT) holdings.[3] This allows the ICE agents and officers to confirm the identity of individuals in encounter situations who are high-interest targets for removal. An alien is considered in this use-case to be of high-interest for removal if they have serious criminal convictions or associations, or if they have a nexus to narcotics trafficking or terrorism. By using the Mobile Fortify app to provide real-time responses to biometric queries, ICE officers and agents can reduce the time and effort to identify targets compared to existing manual processes. Upon submission of photographs and/or fingerprints of (b)(7)(E) the Mobile Fortify app will populate the subject's information (b)(7)(E) including biographical information, original encounter photograph, (b)(7)(E) and derogatory information. In addition to reducing time and effort, this function enhances situational awareness and improves officer safety by providing needed information on the ground during the enforcement effort (b)(7)(E) (b)(7)(E)

ICE does not provide the opportunity for individuals to decline or consent to the collection and use of biometric data/photograph collection. (b)(7)(E) (b)(7)(E) (b)(7)(E) In the case of a photograph, the ICE agent or officer will open the Mobile Fortify app and take a photograph of an individual, which is then used to match against the galleries. The photograph shown (b)(7)(E) is the photograph that was taken during the individual's most recent encounter with CBP, however the matching will be against all pictures CBP may maintain on the individual (b)(7)(E) the Mobile Fortify app will populate with information pulled from the gallery. (b)(7)(E)

For contactless fingerprint collections (which may occur in addition to or in place of the photograph collection), the ICE agent or officer will open the Mobile Fortify app and use their mobile device's embedded camera to take contactless scans of the individual's fingerprints. The Mobile Fortify app will send these scans to ATS, which will then search against the fingerprints pulled from OBIM (b)(7)(E) the Mobile Fortify app will populate with information pulled (b)(7)(E) (b)(7)(E)

[3] DHS/OBIM/PIA-001 Automated Biometric Identification System

Access to the Mobile Fortify app will be limited to ICE agents and officers, as well as some CBP administrative users and select CBP Officers that are assisting with removal operations. The Mobile Fortify app does not retain records on the app itself. It pulls and displays information in real time (b)(7)(E). CBP saves the new photographs and fingerprints, taken using Mobile Fortify, (b)(7)(E) (b)(7)(E) and retained for 15 years, in accordance with the ATS retention schedule. The Mobile Fortify app will be used for identity verification in the field to supplement current processes, however it does not replace ICE's existing procedures at a field office to process an individual.

2. Subjects and Users[4] 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
ICE, and select CBP users	
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
Mobile Fortify app is limited to ICE ERO and HSI users with an operational need to access the app. Some CBP users will also have access for administrative purposes.	

3) Data to be collected

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

The only data directly submitted through the mobile application are biometrics and associated meta data (geolocation). Specifically, through Mobile Fortify, authorized ICE agents and officers will collect a new photograph and, if no match occurs from that photograph, a contactless fingerprint during an encounter using the embedded camera on their government issued mobile device. When that photograph and/or fingerprint is taken, geolocation is tagged to that biometric so ICE can identify where the encounter took place.

While not collected by the Mobile Fortify app, (b)(7)(E) (b)(7)(E) (b)(7)(E) The biographic information displayed includes:

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

Name, DOB, A number, Possible Overstay Status, Possible Citizenship Status, Family members (b)(7)(E) country of citizenship. Metadata: geolocation is collected when the photograph and/or fingerprint is taken, so ICE can identify where the encounter took place.	
b) Does the mobile application collect Sensitive Personally Identifiable Information (SPII)?[5] 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.[6]	
1996 Illegal Immigration Reform and Immigrant Responsibility Act; The Immigration and Nationality Act ("INA"), 8 U.S.C. § 1101, et seq.	
d) Describe *why* this collection of SPII is necessary and the minimum amount of information required to accomplish the purpose of the program.	
This collection allows ICE agents and officers to verify identity (b)(7)(E) (b)(7)(E)	

[5] 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.
[6] Please see DHS Instruction Number: 047-01-009 (Social Security Number Collection and Use Reduction).

e) Does the mobile application collect other types of sensitive content information?[7] Check all that apply.	Location Information[8] ☒ Photos/Videos[9] ☐ Mobile Device ID ☒ Metadata[10] Geolocation is collected on the backend of when a photograph and/or fingerprint was taken, so ICE can know where the encounter took place. ☐ Other. Please list:
f) Describe *why* this collection of sensitive content is necessary to accomplish the purpose of the program.	
metadata: geolocation information is used to identify the physical location of the ICE agent or officer to identify the location where the field intake occurred. **Photos and fingerprints:** Photographs are used along with fingerprints to verify identity (b)(7)(E) (b)(7)(E)	
g) How and where is the information stored? *Please describe below.*	☐ Locally on the mobile device ☒ In a back-end DHS system: ATS ☐ 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.*	
Every new photograph or fingerprint, regardless of match, is an encounter and stored and retained in ATS for 15 years.	
i) How do you ensure that information is disposed of or deleted in accordance with the retention schedule?	
CBP will use the date of encounter on the photographs or fingerprints and the system will do a technical purge and validate deletion using system audit logs to ensure records are deleted in accordance with the ATS data retention period.	
j) Does the project, program, or system retrieve information by personal identifier?	☒ Yes. Please list personal identifiers below. ☐ No.

[7] 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] 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.

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

[10] 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.

Contactless fingerprints, photographs, name, DOB, A number, Possible Overstay Status, Possible Citizenship Status, Family members (b)(7)(E), country of citizenship.

4. Notices

a) Are individuals provided a Privacy Act Statement, Privacy Notice, or some, other type of notice[11] 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.

5. Disclosures

a) Does the mobile application provide "just-in-time"[12] 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.
N/A	
b) Does the mobile application provide any information to other DHS Components or systems?	☒ Yes. CBP and ICE ☐ No.
The Mobile Fortify App collects photographs and fingerprints, (b)(7)(E)	
(b)(7)(E)	
c) Does the mobile application provide any information to third parties (any organization outside of DHS)?	☐ Yes. Please describe. ☒ No.
N/A	

6. Opt-out Features

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

[12] 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[13] 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[14] 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.
No. This mobile application is not public-facing and is only accessible by authorized ICE users. A privacy policy is not requirement for an internal, law enforcement application.	

8. DHS AppVet process?	
a) Has this mobile application been through the DHS AppVet[15] process?	☐ Yes. **Please provide the results of the AppVet with this PTA.** ☒ No.

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

[13] 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.

[14] 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.

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

Component Privacy Office Reviewer:	(b)(6) (b)(7)(C)
Date submitted to Component Privacy Office:	**February 20, 2025**
PRIVCATS ID Number:	(b)(7)(E)
Concurrence from other Components involved (if applicable):	CBP and ICE

(b)(5)

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

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE COMPONENT PRIVACY OFFICE APPROVERS)

CBP Component Privacy Office Approver:	(b)(6) (b)(7)(C) (b)(6) (b)(7)(C) Digitally signed by (b)(6) (b)(7)(C) Date: 2025.05.12 15:28:16 -04'00'
ICE Component Privacy Office Approver:	(b)(6) (b)(7)(C)
PRIVCATS ID Number:	(b)(7)(E)
PTA Approved Date:	May 12, 2025
PTA Expiration Date:	May 12, 2028

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	**No e(3)/Privacy Notice required**
Privacy Policy	**Current Privacy Policy sufficient**
PIA:	**System covered by existing PIA** If covered by existing PIA, please list: DHS/PIA/ICE-015(j) Enforcement Integrated Database (EID), DHS/PIA/CBP-006 Automated Targeting System
SORN:	**System covered by existing SORN** (b)(7)(E) does not contain identifying information of USPERs, so SORN coverage is not required. However, the existing SORN, DHS/CBP-006 Automated Targeting System would cover the collection for anyone covered by the JRA.

Component Privacy Office Adjudication: *Please describe the rationale for privacy compliance determination above.*

Pursuant to the DHS Privacy Policy Guidance Memorandum Number 2025-02, *DHS Privacy Policy Regarding Privacy Threshold Analyses*, effective March 3, 2025, the CBP Privacy Officer has assumed responsibility for the review and adjudication of CBP Privacy Threshold Analyses for compliance with the Privacy Act of 1974 and the E-Government Act of 2002.

Consistent with the DHS Privacy Policy Guidance Memorandum Number 2025-03, *DHS Privacy Policy Regarding Privacy Impact Assessments*, effective March 17, 2025, the CBP and ICE Privacy Officers find that the Mobile Fortify Application is privacy sensitive and requires a Privacy Impact Assessment and a System of Records Notice (SORN).

Although the intended purpose of the Mobile Fortify Application is to identify aliens who are removable from the United States, users may use Mobile Fortify to collect information in identifiable form about individuals regardless of citizenship or immigration status. It is conceivable that a photo taken by an agent using the Mobile Fortify mobile application could be that of someone other than an alien, including U.S. citizens or lawful permanent residents. Therefore a PIA is required pursuant to the E-Government Act.

ICE agents do not know an individual's citizenship at the time of initial encounter and will use the Mobile Fortify mobile application to determine or verify the individual's identity, and confirm that they are a match to the Fortify the Border Hotlist. ICE will receive limited biographic data elements described in #3 via the Mobile Fortify mobile application if the individual encountered matches a photograph from the Fortify the Border Hotlist. Non-matches will not return any additional information. ICE will take no action on individuals who are not a match to the hotlist, unless operational circumstances indicate other violations of law.

The Mobile Fortify mobile application does not retain or store any information locally. However, CBP will retain all photographs, including the non-match photographs (to include U.S. citizens/LPR photographs), as part of ATS holdings consistent with its published ATS PIA and SORN.

The Mobile Fortify mobile application retrieves information via unique identifier, therefore a SORN is also required since citizenship is unknown at the time of collection.

The CBP and ICE Privacy Officers agree that the Mobile Fortify mobile application has sufficient existing PIA and SORN coverage under the following:

1. ICE uses are covered under DHS/PIA/ICE-015(j) Enforcement Integrated Database (EID) PIA. The EID PIA permits ICE to collect and maintain information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and law enforcement investigations and operations conducted by ICE, USCIS, and CBP.
2. CBP uses and storage of all photographs is covered under the DHS/PIA/CBP-006 Automated Targeting System PIA. ATS PIA covers photographs accessible from existing

holdings are photographs captured by CBP during previous entry inspections, photographs from U.S. passports and U.S. visas, immigration records, and photographs from prior DHS apprehensions and encounters.

3. The entire process is covered by the DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297. The ATS SORN covers various types of data and information on travelers and compares it against law enforcement and intelligence databases to identify individuals requiring additional scrutiny. The CBP SORN provides coverage for identity verification until ICE takes any kind of enforcement action, which would be covered by the corresponding ICE SORN.

CBP and ICE Privacy Officers concur that existing privacy documentation is sufficient and grants approval for the Mobile Fortify Mobile Application to collect and maintain personally identifiable information for an additional three years. If any changes occur to the collection or uses of PII, CBP and ICE will update this PTA.