Privacy Impact Assessment

for the

Collection of Advance Information from Certain Undocumented Individuals on the Land Border

DHS Reference No. DHS/CBP/PIA-076

January 19, 2023

Homeland Security

Abstract

Historically, U.S. Customs and Border Protection (CBP) received no advance biographic or biometric information prior to the arrival of undocumented individuals at ports of entry (POE). This lack of information increases the amount of time it takes CBP officers (CBPO) to process undocumented individuals upon their arrival. To streamline and increase processing capacity at land POEs, CBP is expanding the use of the CBP One™ mobile and desktop application to allow the advance submission of biographic and biometric information from undocumented individuals seeking admission into the United States. Undocumented individuals and organizations and entities (e.g., International Organizations (IO) and Non-Governmental Organizations (NGO)) acting on their behalf may voluntarily elect to submit biographic and biometric information via CBP One™. CBP previously provided notice of this advance information collection through a Privacy Impact Assessment (PIA) Update to DHS/CBP/PIA-067(a) Unified Secondary and Privacy Impact Assessment Appendices to the DHS/CBP/PIA-056 Traveler Verification Service[1] and DHS/CBP/PIA-068 CBP One™ Mobile Application.[2] CBP is conducting this new standalone Privacy Impact Assessment to provide full transparency on this initiative and fully assess the risks associated with this collection.

Overview

CBP safeguards America's borders by protecting the public from dangerous people and materials while enhancing the nation's global economic competitiveness by enabling legitimate trade and travel. CBP is charged with ensuring compliance with federal laws at the border including preventing the entry of contraband and other dangerous goods, as well as ensuring that individuals entering the United States comply with all appropriate legal requirements. CBP has authority to inspect, examine, and search persons, vehicles, baggage, and merchandise to ensure compliance with the law.

A citizen of a foreign country who seeks to enter the United States generally must first obtain a U.S. travel document (e.g., a U.S. visa).[3] Possession of a visa does not guarantee admission to the United States; it indicates that the Department of State determined that the

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP ONE™ MOBILE APPLICATION, DHS/CBP/PIA-068 (2021), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[3] A visa is a travel document issued by the traveler's country of citizenship and is placed in the traveler's passport. Certain international travelers may be eligible to travel to the United States without a visa if they meet the requirements for visa-free travel. For example, individuals do not require a visa if they are a citizen or national and traveling from a country that participates in the Visa Waiver Program (VWP) and meet the qualifications of the program.

individual is eligible to seek admission. Upon arrival, all travelers arriving at or traveling through any U.S. air, sea, or land POE are subject to inspection and examination by a CBP Officer and, in some cases, an agricultural specialist.[4] CBP officers perform the inspection to ensure that a traveler is admissible to the United States (as a U.S. citizen or otherwise) and that the traveler is not bringing items into the United States contrary to law.[5] A traveler is not permitted to enter the United States without inspection by a CBPO.

Longstanding regulations require commercial sea and air carriers, as well as private aircraft operators, to submit passenger and crew manifest information to CBP prior to arrival.[6] However, for individuals seeking to enter the United States by land, CBP receives limited or no advance information.[7] For most undocumented individuals[8] who arrive in the United States at a land POE, CBP receives no information about the individuals prior to their arrival.

Advance Information Vetting

When available, CBP uses information obtained in advance from individuals seeking to enter the United States as part of a multi-layered national security approach to conduct appropriate vetting prior to an individual's arrival. Prior to arrival, CBP uses this information to search within CBP's existing information holdings, as well as other law enforcement and national security databases, to determine whether the individual may pose a public safety or national security risk. The advance collection of information also assists in streamlining the inspection process upon an individual's arrival at a POE. CBP has several longstanding advance information collections through which the agency obtains information in advance of arrival either directly from the

[4] *See* 8 CFR Part 235 Inspection of Persons Applying for Admission.
[5] Individuals who are inadmissible are subject to removal from the United States. The Immigration and Nationality Act (INA) sets forth grounds of inadmissibility (INA § 212(a)). The general categories of inadmissibility include health, criminal activity, national security, public charge, lack of labor certification (if required), illegal entry, fraud or misrepresentation, lack of proper documentation, prior removals, unlawful presence in the United States, and several miscellaneous categories. However, for certain grounds of inadmissibility, it may be possible for a person to obtain a waiver of that inadmissibility.
[6] *See* 19 CFR §§ 4.7a, 4.64, 122.22, 122.49a, 122.49b, 122.49c, 122.75a, and 122.75b. CBP uses advance passenger information to vet individuals for public safety and national security concerns. CBP also provides recommendations to air and sea carriers on whether to permit an individual to board. Carriers are not permitted to board or transport individuals who do not possess proper documents.
[7] Rail and bus carriers may voluntarily submit advance passenger information to CBP, although it is not a requirement.
[8] An undocumented individual is an individual who does not possess a valid visa and is not traveling from a country for which the requirement to obtain a visa is waived. Undocumented individuals may or may not possess a passport or other acceptable document that denotes identity and citizenship when entering the United States (e.g., passport, passport card; Enhanced Driver's License; Trusted Traveler Program card (NEXUS, SENTRI, or FAST); U.S. Military identification card; U.S. Merchant Mariner; American Indian Card; or (when available) Enhanced Tribal Card).

traveler (e.g., Trusted Traveler Programs,[9] Electronic System for Travel Authorization (ESTA),[10] Electronic Visa Update System (EVUS)[11]) or from carriers and operators (e.g., Advance Passenger Information[12] and Passenger Name Record[13]).

Undocumented Individuals

As stated above, historically CBP does not receive advance information about undocumented individuals before they arrive at a land POE. Because these individuals do not present a valid travel document,[14] CBP is unable to conduct basic identification verification and standard law enforcement and national security system checks upon arrival as part of CBP's primary inspection. Therefore, undocumented individuals are referred for secondary inspection. During secondary inspection, CBP officers spend significant time collecting, verifying, and manually entering information from undocumented individuals into the Unified Secondary system

[9] Trusted Traveler Programs are risk-based programs that facilitate expedited processing of pre-approved low-risk travelers. CBP offers several types of Trusted Traveler Programs for arrival at air, sea, and land POEs. Eligible travelers who apply for a particular program are vetted against various law enforcement databases, and those who are conditionally approved are interviewed. During the interview, CBP collects biometric information. Trusted Traveler Program members are subject to recurrent vetting to ensure that these travelers do not pose threats to law enforcement or national security and to determine their continued eligibility to receive expedited processing at POEs. Trusted Traveler Programs are generally limited to U.S. citizens, with certain exceptions. *See* DHS/CBP/PIA-002 Global Enrollment System and subsequent updates, *available at* www.dhs.gov/privacy.

[10] The Visa Waiver Program permits eligible travelers from certain participating countries to travel to the United States without first obtaining a visa. Participation in the Visa Waiver Program requires enrollment in CBP's ESTA program. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[11] CBP's EVUS is a web-based enrollment system used to collect information from nonimmigrant noncitizens who 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program and 2) have been issued a U.S. nonimmigrant visa of a designated category. EVUS, similar to ESTA, collects updated information in advance of an individual's travel to the United States. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC VISA UPDATE SYSTEM, DHS/CBP/PIA-033 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[12] In accordance with 19 C.F.R. §§ 122.49a, 122.49b, air carriers are required to send passenger and crew manifests to CBP before an air carrier departs from the foreign port or place for the United States. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM, DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[13] 49 U.S.C. § 44909(c)(3) and its implementing regulation at 19 C.F.R. § 122.49d require air carriers operating flights to or from the United States to provide CBP with certain passenger reservation information, called Passenger Name Record data, to the extent it is collected and contained in the air carrier's reservation and/or departure control systems.

[14] The Department of State and DHS partnered to implement a key 9/11 Commission recommendation and the statutory mandates of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). IRTPA, in part, required the DHS and DOS to develop and implement a plan to require all travelers, U.S. citizens and foreign nationals alike, to present a passport or other acceptable document that denotes identity and citizenship when entering the United States, under the Western Hemisphere Travel Initiative.

(USEC)[15] to document the secondary inspection process from referral to disposition and case processing. Not only is this burdensome for the CBP, but it leads to increased wait times at POEs and reduces the overall CBP throughput.

In an effort to streamline processing of certain undocumented individuals, in May 2021, CBP began collecting advance information from undocumented individuals using CBP One™. Organizations could choose to submit advance information on behalf of an undocumented individual on a voluntary basis. CBP previously provided notice of this advance information collection through a Privacy Impact Assessment Update to DHS/CBP/PIA-067(a) Unified Secondary and Privacy Impact Assessment Appendices to the DHS/CBP/PIA-056 Traveler Verification Service[16] and DHS/CBP/PIA-068 CBP One™ Mobile Application.[17] Since the publication of the Privacy Impact Assessment Update, CBP has expanded the voluntary advance information collection. CBP is documenting the expanded process in this standalone Privacy Impact Assessment to provide full transparency on this initiative and fully assess the risks associated with this collection.

Advance Information Collection

To facilitate the processing of certain undocumented noncitizens at land POEs, CBP created a way for undocumented individuals, as well as organizations and entities who may provide assistance to undocumented individuals, to submit advance information to CBP through CBP One™. CBP One™ is both a mobile and desktop application and serves as a single portal to a variety of CBP services.[18] Individuals may voluntarily choose to submit biographic and biometric information on behalf of themselves and their spouse and children using CBP One™ in advance of their arrival at a POE. Separately, organizations and entities who work with undocumented individuals may collect and transmit the information on behalf of an undocumented individual and their spouse and children in advance of arrival at a POE. In addition to enabling undocumented individuals to submit advance arrival information, CBP is also offering a designated number of dates and times at certain POEs for undocumented individuals to schedule a date and time to

[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR UNIFIED SECONDARY, DHS/CBP/PIA-067, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP ONE™ MOBILE APPLICATION, DHS/CBP/PIA-068 (2021), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[18] The desktop or mobile application is using an intuitive, user-friendly interface and requires no training to use it properly. However, CBP provided multiple live demonstration sessions for designated users as well as provided a Quick Reference Guide. CBP also provided and continues to provide ad hoc assistance to troubleshoot technical issues as well as implement system enhancements to improve the user experience.

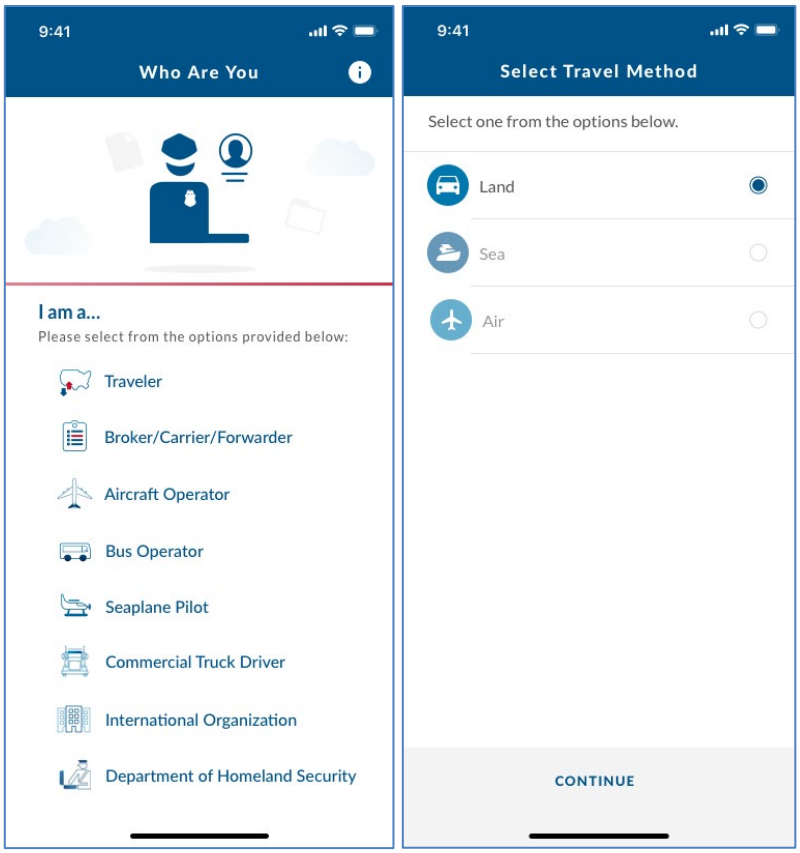
present themselves at the POE for processing.[19]

On January 12, 2023, CBP began accepting advance information submissions from undocumented individuals seeking to travel to the United States through the southwest border (SWB) land POEs to request an exception from 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). "[20] Post-Title 42 Order, this scheduling functionality will be available for undocumented individuals to schedule a time to present themselves at one of the SWB land ports of entry identified above for inspection and processing, rather than arriving unannounced at a port of entry or attempting to cross in-between ports of entry. Post-Title 42 Order, CBP will remove the requirement for individuals to attest to the vulnerability criteria in CBP One™. However, the remainder of the features of the application and scheduling functionality, as described above, will remain the same.

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 port of entry 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.[21]

To submit advance information, individuals and designated personnel/points of contact within organizations and entities ("users") download CBP One™ from the Google Play or iTunes mobile application stores or use a web browser to access the application. Users are prompted to

[19] CBP plans to release a certain number of date/time slots per POE for a given period on a routine basis.
[20] 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.
[21] At the time of publication, the participating POEs are Nogales, Brownsville, Eagle Pass, Hidalgo, Laredo, El Paso (Paso del Norte), Calexico, and San Ysidro.



create a new Login.gov account using an email address, phone number, and password, or sign into an existing Login.gov account to access CBP One™.[22] When users log into CBP One™; users must consent to the CBP Privacy Policy[23] before using the application. Additionally, upon set up, users submitting advance information via the mobile application are required to enable location services[24] on their phone for geolocation purposes.[25]

After logging in, the user is prompted to choose their preferred language and select either "International Organization" or "Traveler" from a list of options, depending on whether the individual is submitting information on their own behalf, or whether a third-party individual, organization, or entity is submitting the information on behalf of a traveler. The user then selects "land" from the travel method options ("land/air/sea"), since the voluntary submission of advance information is limited to land entries and chooses "Continue."

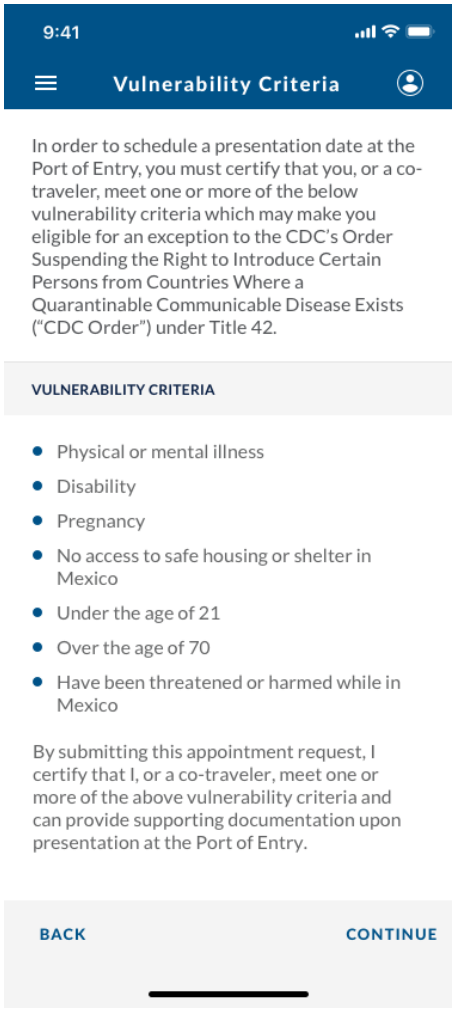
[22] Login.gov ensures a secure connection and identity verification for International Organizations/Non-Governmental Organizations to use CBP One™. *See* GENERAL SERVICES ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR LOGIN.GOV (2020), *available at* https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

[23] The CBP One™ Privacy Policy can be found at https://cbpone.cbp.dhs.gov/#/.

[24] At the time the user submits information to CBP via the CBP One™ mobile application, the GPS on his or her device is pinged by CBP One™. CBP One™ collects and sends the latitude and longitude coordinates to CBP for analytical purposes (e.g., to determine where the user is submitting the advance arrival information from) and to monitor irregularities (e.g., receiving multiple submissions from the same phone), not to conduct surveillance or track user movement. If a user submits information using a web browser, upon submission CBP will collect the Internet Protocol address from the device to monitor for irregularities (e.g., receiving multiple submissions from the same IP address). CBP is implementing geofencing capabilities to limit use of CBP One™ to users within a defined proximity to the United States border. This geofencing is intended to mitigate the likelihood of planned irregular migration to the Southwest Border.

[25] Geolocation is the process or technique of identifying the geographical location of a person or device by means of digital information processed via the internet.

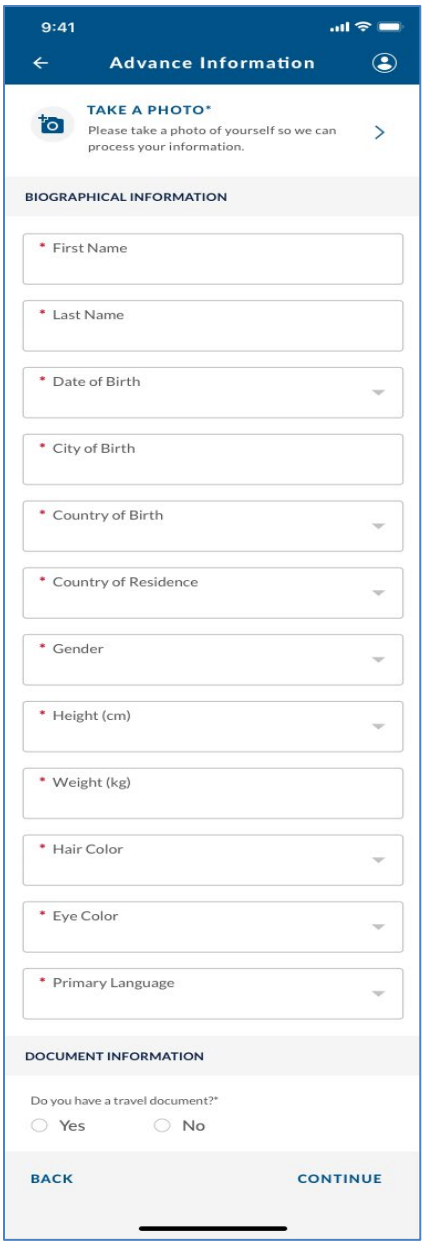
The next screen will then display a list of options, including "Submit Advance Information." After selecting this option, the user is prompted to select their preferred language. After selecting the language, the user is presented with the following list of vulnerability criteria:



- Physical or mental illness;
- 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.

In order to be able to submit advance information to CBP to request an exception to Title 42, the user must attest that they believe that they, or a spouse or child accompanying them, meet the vulnerability criteria. If the user or family member meets the above vulnerability criteria, the user and their family members are permitted to submit advance information to CBP to request an exception from Title 42.

Once the user attests to the vulnerability criteria, the user may submit information on their spouse and children by selecting "Add Individual," if applicable. Once this is selected, the user will be directed to begin entering their and their spouse and children's biographic and biometric information.



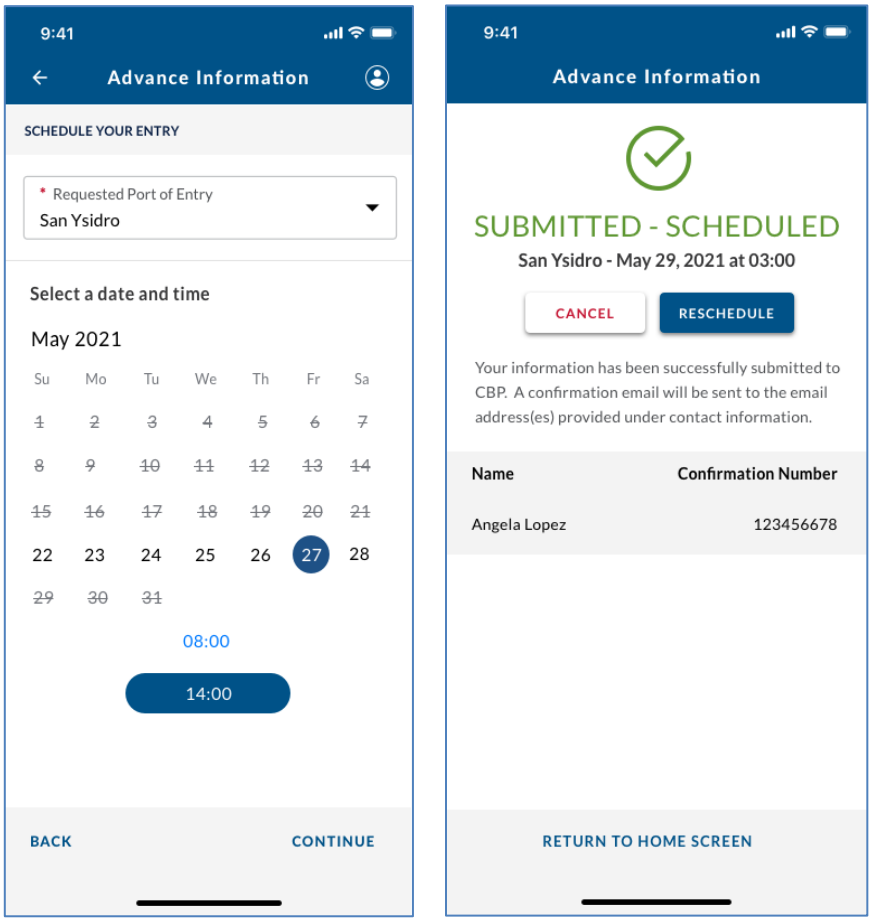
CBP One™ requests the user enter the same information that CBP would otherwise collect from undocumented individuals during the primary and/or secondary inspection, including: name, date of birth, nationality, country/city of birth, country of residence, phone numbers, U.S. address, foreign addresses (optional), employment history (optional), travel history (optional), emergency contact information (optional), family information (optional), marital information (optional), non-Western Hemisphere Travel Initiative (WHTI) compliant[26] identity documents (optional), primary language, gender, height, weight, and eye color.[27]

Once the user enters all requested information, the CBP One™ application prompts the user to either upload a photograph (if using the desktop application) or take a live photo of the undocumented individual (if using the mobile application). All users are required to submit a photograph of the undocumented individual(s) as part of the advance information collection. Biographic advance information cannot be submitted to CBP without including a photograph.

Once the user enters the biographic and biometric (i.e., photograph) information into CBP One™ and enables their location services, the user is required to select a desired POE and desired date/time of arrival, when prompted. The traveler will only be able to request a date and time if they are within a specified distance from the U.S.-Mexico border. CBP requests users to select a desired date/time of arrival, to assist in streamlining the processing upon arrival at a POE. However, CBP treats the selected date and time of arrival as the initial time to present at the POE, and cannot guarantee that an individual will be processed within a particular time frame. In all cases, CBP will inspect and process undocumented individuals in accordance with the POE's capability to do so. The scheduling feature helps CBP to properly allocate resources to the POEs for a given day or week

[26] The types of acceptable Western Hemisphere Travel Initiative compliance documents vary by POE type (i.e., land, air, sea), but generally include U.S. Passport; U.S. Passport Card, Enhanced Driver's License, Enhanced Tribal Card, Trusted Traveler Program card (NEXUS, SENTRI or FAST); U.S. Military identification card when traveling on official orders; U.S. Merchant Mariner document when traveling in conjunction with official maritime business.
[27] The data elements are substantially similar to, and used for the same purposes as, the Form I-94W Nonimmigrant Visa Waiver Arrival/Departure Record.

to further assist in streamlining in-person processing upon arrival. Once a POE and desired date/time of arrival is selected, the user may submit the information to CBP. Upon submission, the user is presented with a confirmation screen which displays a confirmation number along with the selected POE and date/time, if applicable. A copy of the confirmation is also sent to the email address provided as part of the advance information collection process. The granting of an appointment does not guarantee an exception from the Title 42 Order, nor does it guarantee admission into the United States. CBP officers make determinations of whether an exception is authorized, as well as all admissibility determinations at the POE. CBP officers consider all available information, including information supplied in advance by the traveler, and the totality of the individual case circumstances and will determine the appropriate processing disposition for each individual.



The submission of advance information through the CBP One™ application is voluntary. Once the Title 42 Order is no longer in effect, individuals may present themselves at a port of entry for processing without utilizing CBP One™. However, if an individual chooses to not submit advance

information and schedule their arrival, they may experience a longer wait time than individuals who submitted their information in advance. In all cases, CBP will continue to process all travelers who present themselves for inspection as quickly as possible.

CBP Collection and Use Prior to Arrival

When a traveler uses CBP One™ to submit advance information, the biographic information and photograph is transferred to a segregated database within the Automated Targeting System (ATS).[28] CBP then conducts biographic and biometric pre-arrival vetting against ATS's Unified Passenger (UPAX). UPAX, an ATS functionality, processes submitted information against information within CBP holdings and applies risk-based rules centered around CBP officer experience, analysis of trends of suspicious activity, and raw intelligence from DHS and other government agencies. Pre-arrival vetting enables CBP to identify any previous DHS encounters, public safety threats (such as wants/warrants), and national security threats (such as links to terrorist organizations). Pre-arrival vetting individuals for public safety and national security concerns reduces the amount of time that officers typically spend on determining whether the individual is a match to checks and results completed during the inspection process. CBP does not conduct pre-arrival vetting to pre-determine an individual's processing disposition nor admissibility to the United States.

In addition to conducting pre-arrival vetting, CBP also creates a templatized copy of the photograph in a standalone Traveler Verification System (TVS) gallery.[29] CBP stages all photographs submitted via CBP One™ in a segmented TVS gallery until the individual arrives at the POE. CBP temporarily retains the photographs of undocumented individuals within TVS for 1 year after submission for identity confirmation, evaluation of the technology, assurance of accuracy of the algorithms, and system audits.

As noted above, the user is required to select a POE and desired date and time on which the undocumented individual(s) intends to arrive in order for the submission to be complete. If the user does not select a POE and desired date and time as part of the original submission, the user may retrieve the submission using the confirmation number to select a POE and desired date and

[28] *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) (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[29] CBP's TVS is an accredited information technology system consisting of a group of similar systems and subsystems that support the core functioning and transmission of data between CBP applications and partner interfaces. Since early 2017, CBP has used the TVS as its backend matching service for all biometric entry and exit operations that use facial comparison, regardless of air, land, or sea. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

time at a later date. The user can also retrieve the submission to reschedule an undocumented individual's arrival date and time.

CBP Inspection Process

Undocumented noncitizens who utilize CBP One™ to submit advance information will generally be processed in a more streamlined manner than individuals who do not utilize the app, since CBP is able to pre-populate the advance information into CBP systems which ultimately reduces the amount of manual data entry that is typically completed during the inspection process.[30] Post-Title 42 Order, CBP estimates that the importation of information collected in advance of arrival at the POE will result in a savings of 16 minutes in CBP's processing of each undocumented individual.

Primary Inspection

All individuals are subject to primary inspection upon arrival at the POE. At the beginning of the primary inspection process, the CBP officer takes a photograph, using Simplified Arrival, a system that uses biometric facial matching or biographic matching, to locate and display relevant records CBP maintains on the individual.[31] Using a designated processing mode in Simplified Arrival, the individual's photograph is compared against the pre-staged gallery of images taken from the photographs submitted via CBP One™ directly from the individual or by the organizations and entities, known as *1:n matching*. If TVS does not produce a match, CBP officers may query the segregated database using the CBP One™ confirmation number or name, date of birth, and country of citizenship provided by the undocumented individual. Once an individual is matched and all primary inspection checks are complete, CBPOs use Simplified Arrival to generate a referral for the undocumented individual to go to secondary inspection.[32]

Secondary Inspection

Advance information submitted via the CBP One™ application streamlines the secondary inspection process by pre-populating biographic information in USEC. When a CBP officer refers

---

[30]. Undocumented individuals who do not submit advance information may still be processed at a POE, but may need to wait in line with other undocumented individuals for which CBP does not have advance information for, and will likely experience longer wait and processing times.

[31] Simplified Arrival is an enhanced international arrival process that uses facial biometrics to automate the manual document checks that are already required for admission into the United States, providing individuals with a secure, touchless travel experience while fulfilling a longstanding Congressional mandate to biometrically record the entry and exit of non-citizens. *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.

[32] If an individual arrives at a POE without sufficient documentation, as part of standard processing the CBPO typically refers the individual for a secondary inspection.

an undocumented individual for secondary inspection, they have the option of importing the biographic information submitted in advance via CBP One™ in the corresponding USEC referral event via the segregated backend database where it is stored in ATS. A CBP officer reviews the imported information, verifies the accuracy of the data, and makes any necessary updates to the event. The USEC event may include the confirmation number previously generated by CBP One™.[33] CBP officers may also manually add the individual's CBP One™ confirmation number as a record ID in USEC. The USEC event for the undocumented individual includes the previously submitted biographic information, any biometric information, and the UPAX pre-arrival and primary vetting results. The results of pre-vetting will display relevant events/encounters that the CBP officers will use to inform questioning that typically occurs as part of the secondary inspection. The results may also lead CBPOs to conduct additional system checks in accordance with standard secondary processes.

CBP officers determine an individual's admissibility and appropriate processing disposition on a case-by-case basis and consider the totality of the facts and circumstances known to the officer at the time of inspection. CBPOs do not make any disposition determinations in advance of an encounter with an undocumented individual.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Undocumented individuals (either on their own behalf or through organizations and entities) may submit information to CBP on a voluntary basis, for the purpose of facilitating and implementing CBP's mission. This collection is consistent with DHS and CBP's authorities, including under 6 U.S.C. §§ 202 and 211(c). Under these authorities, DHS and CBP are permitted to maintain the security of the border, including "securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States," and "implement[ing] screening and targeting capabilities, including the screening, reviewing, identifying, and prioritizing of passengers and cargo across all international modes of transportation, both inbound and outbound." Providing advance information in CBP One™ does not create or confer any rights, substantive or procedural, enforceable by law by any party in any matter, whether civil or criminal. It places no legal requirements on CBP nor any other government agency or department; has no regulatory effect; confers no remedies; and does not have the force of law or a ruling of any administrative agency, court, or other governmental entity.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply

[33] The CBPO uses the following information to create the referral: first name, last name, date of birth, nationality, confirmation number, document type and number (if available), issuing country, and photograph.

to the information?

The ATS System of Records Notice (SORN)[34] covers the collection of information in advance of travel from undocumented individuals. All information collected from travelers at the time of inspection and processing is covered by the Nonimmigrant Information System[35] and TECS[36] System of Records Notices. Additionally, the Arrival Departure Information System (ADIS) System of Records Notice permits CBP to collect information from certain public and private organizations regarding individuals who seek entry or admission into the United States.[37]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. All CBP source systems have undergone the Security Authorization process in accordance with DHS and CBP policy, which complies with federal statutes, policies, and guidelines. ATS, as a system that stores advance information from undocumented individuals, received a renewed Authority to Operate on January 26, 2020.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

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.[38]

---

[34] *See* DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297, *available at* https://www.dhs.gov/system-records-notices-sorns.
[35] *See* DHS/CBP-016 Nonimmigrant Information System, March 13, 2015, 80 FR 13398, *available at* https://www.dhs.gov/system-records-notices-sorns.
[36] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778, *available at* https://www.dhs.gov/system-records-notices-sorns.
[37] *See* DHS/CBP-021 Arrival and Departure Information System, November 18, 2015, 80 FR 72081, *available at* https://www.dhs.gov/system-records-notices-sorns.
[38] EID is a DHS shared common database repository used by several DHS law enforcement and homeland security

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

CBP previously received emergency approval from the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA) for the collection of advance information from undocumented individuals who seek to enter the United States under OMB 1651-0140.[39] This approval was limited to the collection of advance information from certain undocumented individuals potentially amenable for an exception to Title 42 at southwest border land POEs. CBP is now concurrently seeking a separate emergency approval for the collection of advance information from all undocumented individuals. The 60-day notice for the extension and amendment published on September 28, 2021, and CBP is now seeking approval by OMB to extend and amend this collection under the Paperwork Reduction Act.[40]

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

To streamline processing at POEs, CBP is collecting voluntarily submitted biographic and biometric information in advance of arrival from certain undocumented individuals . This information is expected to streamline processing upon arrival. This voluntary information collection is completed through the CBP One™ application by, or on behalf of, the undocumented individual. This advance collection enables CBP to streamline in-person processing upon arrival by reducing the inspection and administrative burden for both CBP officers and the undocumented individual.

CBP One™ collects the following information from undocumented individuals:

- Name;
- Date of birth;

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.

[39] *See* https://omb.report/omb/1651-0140.

[40] 86 FR 53667 (September 28, 2021).

- Phone number(s);
- U.S. address;
- Country/City of Birth;
- Country of Residence;
- Foreign address(es) (optional);
- Nationality;
- Employment history (optional);
- Travel history (optional);
- Emergency contact information (optional);
- Family information (optional);
- Marital information (optional);
- Non-Western Hemisphere Travel Initiative (WHTI) compliant identity documents (optional););
- Gender;
- Height;
- Weight;
- Eye color;
- Preferred language;
- Requested Date/Time of Arrival (required to schedule);
- Intended Arrival POE (required to schedule); and
- Photograph (required for submission).

Undocumented individuals and organizations and entities who submit information to CBP via CBP One™ on behalf of such individuals are required to provide a photograph of the undocumented individual as part of the advance information package. Users may upload an existing photograph if using the desktop application or capture a live photograph through CBP One™ if using the mobile application. Advance information cannot be submitted to CBP without the inclusion of a photograph.

In addition to the information collected about undocumented individuals, CBP also collects limited information about the third-party who is submitting information on behalf of an

undocumented individual. CBP requests that the third-party representative submits the following information: first name, last name, and email address.

2.2 What are the sources of the information and how is the information collected for the project?

Information is collected directly from an individual or representative (e.g., spouse, parent, organization) who submits information on behalf of the individual. Information is submitted through the CBP One™ mobile or desktop application.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

CBP collects this information directly from the undocumented individual or from organizations and entities submitting the information on behalf of the individual. While there is always an inherent risk to manual data entry, organizations, entities, and the individuals themselves can review and verify the information prior to submission to CBP. Moreover, during the inspection process, a CBPO will verify and update any information in USEC that is incorrect or inaccurate.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of overcollection, since CBP may collect advance information about individuals who do not actually arrive at the POE.

Mitigation: This risk is partially mitigated. CBP is collecting this information from individuals who are seeking to travel to the United States. The undocumented individuals voluntarily provide this information directly to CBP via CBP One™ or through organizations and entities who submit the information to CBP via CBP One™ on the undocumented individual's behalf. Advance information helps to streamline the individual's inspection and processing upon their arrival at a POE. This information collection is similar to other advance information collections, such as Advance Passenger Information (API) data,[41] where a commercial travel carrier submits certain advance information on passengers intending to travel to the United States. In this circumstance, CBP also collects and retains information on individuals who may intend to

[41] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM, DHS/CBP/PIA-001 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

travel but fail to board the carrier. Another example is the CBP Advance Travel Authorization (ATA) process,[42] under which CBP collects certain information from individuals as part of the process of determining whether they are eligible to obtain advance authorization to travel to the United States to seek a discretionary grant of parole. In this circumstance, the traveler may not end up traveling to the United States. In all circumstances, CBP uses the advance information, combined with the results of the pre-arrival vetting to identify public safety threats (such as wants/warrants) and national security threats (such as links to terrorist organizations). Furthermore, for future travel, CBP officers may refer to past vetting results as a basis for interview inspection questions and to inform processing dispositions or admissibility determinations.

Privacy Risk: There is a risk that information submitted via CBP One™ and stored in ATS will be inaccurate.

Mitigation: This risk is mitigated. While there is always an inherent risk to manual data entry, CBP One™ users can review and verify the information prior to submission to CBP. Once an individual arrives at the POE, advance information also reduces the potential for manual data entry error by pre-populating the USEC event with information previously submitted on behalf of the undocumented individual. CBPOs then verify the information with the undocumented individual during processing and can make any changes if necessary.

Privacy Risk: There is a risk that CBP is collecting more information than necessary to make an admissibility determination and determine the appropriate processing disposition.

Mitigation: This risk is mitigated. CBP is collecting the same information that is typically collected prior to an individual traveling to the United States (e.g., APIS, ATA, Passenger Name Record data,[43] ESTA,[44] Form I-94 *Nonimmigrant Visa Waiver Arrival/Departure*[45]). Additionally, the information collected in advance of an undocumented individual's arrival is consistent with the information that CBP normally collects at the POE during secondary inspection in accordance

[42] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE TRAVEL AUTHORIZATION, DHS/CBP/PIA-073, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[43] U.S. law requires air carriers operating flights to, from, or through the United States. to provide CBP, with certain passenger reservation information, called Passenger Name Record data. The collection of Passenger Name Record data allows CBP to prevent, detect, investigate, and prosecute terrorist offenses and related crimes and certain other crimes that are transnational in nature. Air carriers are required to provide this information on all persons traveling on flights to, from, or through the United States to CBP beginning 72 hours prior to departure of a flight, and up until 24 hours before the scheduled flight departure.

[44] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[45] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE I-94 WEBSITE APPLICATION, DHS/CBP/PIA-016 (2013 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

with existing CBP processes. The advance collection of this data streamlines the processing of these individuals upon their arrival to the POE because it reduces manual data entry into the USEC event. Providing advance information to CBP is not a prerequisite for undocumented individuals to be processed at a POE.

Privacy Risk: There is a risk that CBP will be unable to process the application without the user providing all requested information.

Mitigation: This risk is mitigated. Should an individual seek to use this process, CBP has designated certain advance information fields and questions as mandatory. Users who fail to complete mandatory fields are unable to submit the advance information to CBP. However, the user is not required to supply certain information if it is not relevant. For example, if a user answers "Yes" to the question asking if they are employed, they are presented with additional fields to complete. If the user responds with "No," they will not be presented with or required to provide employment related information. The only required field under the mandatory questions is when a user indicates "Yes" to travel documents, they must input the document type, number, and country of issuance. If a user fails to appropriately respond to the questions (e.g., answers "No" to travel documents, when they should have answered "Yes"), this will cause delays in processing and the individual will likely spend additional time in secondary inspection upon arrival at a POE.

Privacy Risk: There is a risk of overcollection now that CBP requires the submission of photograph with the advance information package.

Mitigation: This risk is partially mitigated. As noted above, post-Title 42 Order, providing advance information to CBP will not be a prerequisite for undocumented individuals to be processed at a POE. Undocumented individuals who voluntarily provide this information to CBP (directly or through organizations and entities) are expected to be processed in a more streamlined manner upon their arrival to a POE. Should an undocumented individual choose to submit advance information to CBP, they must supply a photograph as part of the submission. The advance submission of a photograph provides CBP officers with a mechanism to confirm upon arrival that the undocumented individual as a match to information submitted in advance. Therefore, upon arrival at a POE, the officer will visually compare the photograph submitted via CBP One™ against the individual physically present at the POE who is seeking admission to the United States. This manual verification will help ensure that the CBP officer is processing the correct person, ultimately reducing the potential for fraud. In addition to the manual verification, CBP the conducts the 1:n matching, as described above.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP uses advance information collected from certain undocumented individuals via CBP

One™ to streamline processing upon arrival at the POE. The advance information collection is a combination of biographic and biometric information, to include the individual's selected POE and requested date/time of arrival. The purpose of this advance collection is to achieve efficiencies in processing individuals upon their arrival at the POE. The advance collection of scheduling information allows CBP to appropriately allocate resources to those POEs and dates/times at which undocumented individuals have requested to arrive.

Upon submission of advance information through CBP One™, the advance information is staged within ATS' UPAX for pre-arrival and primary vetting results. CBP uses the undocumented individuals' advance information to perform pre-arrival vetting, including queries of certain databases to identify any previous DHS encounters, public safety threats (such as wants/warrants), and national security threats (such as links to terrorist organizations) prior to an undocumented individual's arrival at a POE. Pre-arrival vetting for public safety and national security concerns reduces the amount of time that officers typically spend on determining whether the individual is a match to checks and results completed during the inspection process. CBP does not conduct pre-arrival vetting to pre-determine an individual's admissibility to the United States or to pre-determine a particular processing disposition.

CBP uses the photographs submitted via CBP One™ as part of the advance information to build a segmented TVS gallery. CBP stages all photographs submitted via CBP One™ in this segmented TVS gallery until the individual arrives at the POE. Once the individual arrives at a POE, the officer uses the photograph provided though CBP One™ to confirm the individual as a match to information submitted in advance of arrival. CBPOs complete this manual identity matching to reduce the potential for fraud.

In addition to the photograph provided through CBP One™, the CBP officer takes a new live photograph of the individual upon arrival at the POE. Using Simplified Arrival, the undocumented individual's live photograph is compared against the pre-made gallery of images taken from the photographs submitted via CBP One™ — known as 1:n matching. If TVS does not produce a match, CBP officers may query the segregated database using the CBP One™ confirmation number or name and date of birth provided as part of the advance information package. Following basic primary checks and standard biometric searches and enrollment, CBPOs use Simplified Arrival to generate a referral for the undocumented individual to go to secondary inspection.[46]

CBP officers may import the advance information into a USEC event. This helps to streamline processing and reduces the need to manually enter information into USEC. Additionally, CBPOs access the UPAX pre-arrival vetting results via USEC. The results include

[46] If an individual arrives at a POE without sufficient documentation, as part of standard processing, the CBPO typically refers the individual for a secondary inspection.

relevant events/encounters that the officers may use to inform questioning that typically occurs as part of the secondary inspection. The results may also lead them to conduct additional system checks. Once the inspection is complete, the CBP officer will make appropriate processing and admissibility determinations based on the totality of the circumstances.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. ATS is used to compare existing information about travelers and cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence.

3.3 Are there other components with assigned roles and responsibilities within the system?

The advance information is stored in a segmented ATS database and is typically not available for access by other DHS components. However, if CBP creates a UPAX event based on pre-arrival vetting, the UPAX event will be accessible by DHS components who have access to the Targeting Framework within ATS. Furthermore, upon the individual's arrival at a POE, the advance information may be imported into USEC. While the roles and responsibilities in USEC are limited to CBP personnel only, other DHS components may create TECS lookouts to aid in referring a traveler to secondary inspection. Furthermore, secondary inspections that result in adverse or administrative immigration actions are automatically sent to and stored in the ICE EID as immigration events. Additionally, biometric and associated biographic information collected during the secondary inspection process is enrolled in the Automated Biometric Identification System/Homeland Advanced Recognition Technology System (IDENT/HART).[47]

3.4 Privacy Impact Analysis: Related to the Uses of Information

[47] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim..pdf. DHS is in the process of replacing IDENT with the Homeland Advanced Recognition Technology System (HART) as the primary DHS system for storage and processing of biometric and associated biographic information. For more information about HART, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

Privacy Risk: There is a risk that CBP will conduct pre-arrival vetting checks on individuals who do not arrive in the United States.

Mitigation: This risk is partially mitigated. CBP may conduct pre-arrival vetting on undocumented individuals who never arrive in the United States. This use is consistent with current CBP operations, such as when CBP receives Advance Passenger Information from carriers who submit information regarding travelers intending to travel to the United States but who do not arrive. In both these circumstances, CBP still collects information on and vets travelers to identify public safety threats (such as wants/warrants) and national security threats (such as links to terrorist organizations). Additionally, CBP is collecting this information through CBP One™ on a voluntary basis. When an individual submits the information on behalf of themselves, CBP One™ presents them with a Privacy Policy prior to collecting advance information. By acknowledging the policy and submitting information through CBP One™, the individual consents to CBP's use of their information, to include pre-arrival vetting and screening.

Furthermore, similar to Advance Passenger Information, CBP only retains advance information submitted through CBP One™ for 1 year in a segregated backend database within ATS and TVS. Therefore, in most circumstances, if the individual does not arrive at a POE within 1 year of providing information, CBP will delete the data and cannot use the advance information beyond the original intended purpose of streamlining processing upon arrival. However, in circumstances where CBP finds derogatory information and creates a UPAX event during pre-arrival vetting, CBP will store the information in ATS for 15 years, consistent with the ATS retention schedule.

Privacy Risk: There is a risk that CBP will use the information for purposes other than what is stated in this Privacy Impact Assessment.

Mitigation: This risk is mitigated. The original DHS/CBP/PIA-067 CBP Unified Secondary and this Privacy Impact Assessment update articulate the ways in which CBP will use the information and the mechanisms in place to ensure it does so. Once the information from CBP One™ is populated into a USEC event, CBP will use the information in the same way that CBP uses and shares information in other USEC events. Secondary inspections that result in adverse or administrative immigration actions are automatically sent to and stored in ICE EID. Consistent with standard operating procedures, the individual's biometric and associated biographic information collected during the secondary inspection process will also be enrolled in IDENT/HART.

Privacy Risk: There is risk that geolocation information (e.g., latitude, longitude) collected from users of certain CBP One™ functions may be used by CBP to conduct surveillance on the undocumented individual or to track their movement.

Mitigation: This risk is mitigated. The geolocation information collected through CBP One™ is not used to conduct surveillance or track user movement. CBP does not know the location of the user's device beyond the moment of submission of the data. At the time the user submits their advance arrival information, the device's GPS is pinged by CBP One™, and the latitude and longitude coordinates are sent to CBP. The response to the GPS ping is only collected at the exact time the user pushes the submit button and is used to confirm the device is within the CBP-determined appropriate proximity to the U.S. border. The latitude and longitude information captured is not visible to CBP officers. CBP collects the latitude and longitude information from the GPS ping to permit an individual to submit their advance arrival information. If the individual is not within the defined radius, they are unable to submit advance arrival information.

Privacy Risk: There is a risk that CBP will enroll undocumented individuals in IDENT/HART based on the photograph submitted via CBP One™.

Mitigation: This risk is mitigated. CBP uses the CBP One™ photograph to conduct one-to-many (1:n) vetting against derogatory photographic holdings in ATS for law enforcement and national security concerns and to create the TVS gallery of CBP One™ photographs. The CBP One™ photographs are stored in a segmented database within TVS and ATS. CBP populates the segmented TVS gallery with images sent to CBP from CBP One™. However, upon arrival at a POE, CBP officers take another photograph of the individual, and the photograph collected through CBP One™ is deleted from TVS within 1 year of submission. The photograph that is taken by the CBPO at the POE is enrolled into IDENT/HART, as it is a biometric travel encounter.

Privacy Risk: There is a risk that individuals who do not have access to a desktop or mobile device or understand how to submit information via the CBP One™ application will be treated differently than those who voluntarily submit advance information.

Mitigation: This risk is partially mitigated. While there is a possibility that undocumented individuals may not have access to a computer or mobile device to submit information in advance to CBP, organizations and entities can also provide advance information to CBP on behalf of undocumented individuals. Furthermore, the submission of advance arrival information is voluntary. Undocumented individuals seeking to travel to the United States may choose to work with International Organizations and Non-Governmental Organizations to submit information to CBP through CBP One™.

Privacy Risk: There is a risk that CBP will use the photograph beyond the purposes described in this PIA.

Mitigation: This risk is mitigated. CBP collects and uses the photograph for the following purposes:

1. To conduct one-to-many (1:n) vetting against derogatory photographic holdings in ATS;

2. To populate the pre-staged TVS gallery;
3. To compare the photograph taken during the primary inspection via Simplified Arrival against the pre-staged gallery of CBP One™ photographs; and,
4. To ensure the user is within a prescribed proximity to the border to schedule their arrival.

As part of the vetting process, CBP uses the CBP One™ photograph to biometrically vet the photograph against ATS holdings. The purpose of this vetting is to identify national security and law enforcement concerns. CBP uses the photograph submitted via CBP One™ to build a segmented TVS gallery. CBP stages all photographs submitted via CBP One™ in this segmented TVS gallery until the individual arrives at the POE. Once the individual arrives at a POE, the CBPO uses the photograph provided though CBP One™ to confirm the individual is a match to Simplified Arrival photograph. Finally, CBP may also utilize the live photograph combined with geolocation to ensure users are in a prescribed proximity to the border to schedule their presentation date and time with CBP. Once the user enables location services on their phone, CBP can rely on the geofencing[48] capabilities within the photograph to ensure mobile device is being used by a "live person" who is requesting to schedule their arrival at a POE.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CBP One™ provides users with a Privacy Notice prior to the collection of information. CBP is providing general notice on the expansion through this Privacy Impact Assessment. CBP previously issued an update to the DHS/CBP/PIA-067(a) Unified Secondary Privacy Impact Assessment and appendices to DHS/CBP/PIA-056 Traveler Verification Service and DHS/CBP/PIA-068 CBP One™ Mobile Application. On May 3, 2021, OMB granted emergency approval for the collection of advance information from certain undocumented individuals seeking an exception to Title 42 under the Paperwork Reduction Act. CBP is now seeking approval from OMB to extend and amend this collection.[49]

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Advance information about undocumented individuals is provided to CBP through CBP One™ on a voluntary basis. Post-Title 42 Order, providing advance information to CBP will not

[48] A geo-fence is a virtual geographic boundary, defined by CBP personnel, that determines a person or devices proximity to a designated area or location.
[49] 86 FR 53667 (September 28, 2021).

be a prerequisite for undocumented individuals to be processed at a POE. By providing this information to CBP, individuals consent to CBP's use of the information for pre-arrival vetting purposes, and for purposes of streamlining their processing upon arrival. If an undocumented individual does not provide information in advance, the individual will be inspected and processed in accordance with a POE's capabilities to do so; thus, the individual may need to wait longer to be inspected, and it may take longer for CBP to process them.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that undocumented individuals who use the assistance of others (e.g., organizations) will not receive notice as they do not directly log in to CBP One™.

Mitigation: This risk is partially mitigated. CBP will provide direct notice to individuals who submit information on their own behalf. In instances where an organization is submitting information on behalf of an undocumented individual, CBP will not be able to provide direct notice to the individual whose information CBP is collecting. As noted above, CBP has communicated this initiative through various means including an update to DHS/CBP/PIA-067 and DHS/CBP/PIA-068. CBP is also issuing this standalone Privacy Impact Assessment to provide transparency and describe the privacy risks and mitigations associated with the proposed changes to the collection of advance information.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

The advance information collected via CBP One™ will be stored in a segregated database within ATS for 1 year. However, if the advance information is imported into a USEC event, or a UPAX event is created during pre-arrival vetting, it will be stored within ATS for 15 years consistent with the ATS retention schedule. Additionally, the USEC event data will be transmitted into and stored in other systems, where it is retained in accordance with the retention schedules for those systems. For example, all USEC information, regardless of a positive or negative outcome, is sent to and stored in TECS where it is retained for 75 years in accordance with the TECS retention schedule. Many of the forms completed through USEC are sent to the ICE EID as the source system, in which case they are stored for 75 years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that CBP will retain information on individuals who do not arrive in the United States.

Mitigation: This risk is partially mitigated. CBP is retaining information on individuals who may not arrive in the United States. However, CBP is retaining this information on a temporary basis for 1 year, which is consistent with the APIS System of Records Notice. If the

undocumented individual does not appear at a POE within a year of providing advance information via CBP One™, CBP will purge the data—unless CBP finds derogatory information and creates a UPAX event during pre-arrival vetting. If CBP creates a UPAX event, CBP will store the information in ATS for 15 years consistent with the ATS retention schedule.

Privacy Risk: There is a risk that the CBP One™ application itself will retain advance information.

Mitigation: This risk is mitigated. CBP One™ is a single portal to a variety of CBP services. Regardless of the service, CBP One™ does not store any information locally on the device. CBP pushes all information collected through CBP One™ to back-end systems. No information is stored locally on the undocumented individual or representative's device or in the CBP One™ application itself. The retention of information CBP collects through CBP One™ depends on the respective CBP One™ service. As described above, for this service, CBP is storing the advance information collected via CBP One™ in a segregated database within ATS for 1 year. Any information that is transferred into subsequent systems will be stored pursuant to their own retention schedules. CBP has analyzed the application to ensure that information is sent only to CBP, and the application can only access the information necessary to complete the respective service.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Advance information that is imported into CBP systems may be shared on a case-by-case basis with appropriate federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, or when CBP believes the information would assist enforcement of civil or criminal laws. The information entered into CBP One™ and temporarily stored in the segregated ATS database and TVS is not shared outside of CBP. However, once information becomes an immigration event in USEC, USEC disseminates the event information to various transactional systems that are accessed and used by counterterrorism, law enforcement, and public security communities. This information may reveal information about suspected or known violators of the law and other persons of concern. CBP only shares information consistent with the published routine use(s) in the relevant System of Records Notice(s).

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

CBP shares immigration events with external organizations consistent with the published routine uses in the System of Records Notices, which are compatible with the original purpose of collection.[50] CBP details data sharing practices in Memoranda of Understanding/Agreement (MOU/A) and Interconnection Security Agreements (ISA), which govern sharing data outside of CBP, when appropriate. Under the terms of these Memoranda of Understanding/Agreement and Interconnection Security Agreements, other agencies are required to secure CBP information consistent with approved security practices that meet DHS standards. Recipients from other agencies are required by the terms of the relevant information sharing agreement to employ security features to safeguard the shared information.

6.3 Does the project place limitations on re-dissemination?

Yes. CBP implements Memoranda of Understanding/Agreement with external organizations prior to the systematic sharing of information. When sharing information with parties outside of DHS, the same specifications related to security and safeguarding of privacy-sensitive information that are in place for CBP are applied to the outside entity. Any agreements between CBP and external entities fully outline responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination, prior to information sharing. Access to records is governed by need-to-know criteria that demand that the receiving entity demonstrate the mission-related need for the data before access is granted. In the terms of a negotiated agreement or the language of an authorization providing information to an external agency, CBP includes a justification for collecting the data and an acknowledgement that the receiving agency will not share the information without CBP's permission, as applicable. Information that is shared with other agencies, federal, state, local, tribal, or foreign, outside of the context of any Memoranda of Understanding/Agreement or prior written agreement generally requires a written request by the requesting agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Memoranda of Understanding/Agreement and other written agreements defining roles and responsibilities are executed between DHS and each agency that receives CBP data on a systematic basis. The information may be transmitted either electronically or as printed materials to

[50] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008); DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012); DHS/CBP-013 Seized Assets and Case Tracking System, 73 FR 77764 (December 19, 2008); DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (October 19, 2016); DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69983 (September 18, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.

authorized personnel. Electronic communication with other non-CBP systems may be enabled via message/query-based protocols delivered and received over secure point-to-point network connections between CBP systems and the non-CBP system. CBP's external sharing of the data recorded in USEC complies with statutory requirements for national security and law enforcement systems.

Information that is shared with other agencies, federal, state, local, tribal, or foreign, outside of the context of any Memoranda of Understanding/Agreement or other prior written arrangement generally requires a written request by the agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office and documented in DHS Form 191.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that advance information that is stored within TVS and ATS will be shared externally.

Mitigation: This risk is mitigated. Upon receipt, CBP stages all photographs submitted via CBP One™ in a segmented TVS gallery until the individual arrives at the POE. CBP temporarily retains the photographs of undocumented individuals within TVS for 1 year after submission for identity confirmation, evaluation of the technology, assurance of accuracy of the algorithms, and system audits. TVS does not share information with external partners. Additionally, the CBP One™ data is sent to and stored in a segregated database in ATS. This segregated database is a separate set of independently managed tables within ATS and will not be shared externally. However, once the CBP One™ data is imported into USEC as an event, due to a referral to secondary inspection, CBP shares the information externally on an as needed basis, as described above. Furthermore, once an immigration event is created, the information can be queried from targeting or secondary systems to which external partners may have access. The data will not be accessible by external entities until the CBP officer imports the information into USEC when the individual arrives at the POE.

Privacy Risk: There is a risk that advance information included as part of immigration events will be inappropriately shared to external partners.

Mitigation: This risk is partially mitigated. When sharing immigration events with parties outside of DHS, the same specifications related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to this information is governed by a need-to-know criterion that demands the receiving entity demonstrate the mission-related need for the data before access is granted. The reason for the access, a specific mission purpose, and an intended use consistent with the receiving agency's purpose and CBP's justification for collecting the data are also concerns that are included in either the terms of negotiated Memoranda of

Understanding/Agreement and Interconnection Security Agreements or the language of an authorization providing facilitated access to an external agency. The Memoranda of Understanding/Agreement specify the general terms and conditions that govern the use of the functionality or data, including limitations on use. Interconnection Security Agreements specify the data elements, format, and interface type, including the operational considerations of the interface. Memoranda of Understanding/Agreement and Interconnection Security Agreements are periodically reviewed, and outside entities must agree to use, security, and privacy standards before sharing can continue.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

The CBP One™ application does not store any information; therefore, there are no records to correct or amend within CBP One™. If an undocumented individual submits incorrect information through CBP One™ they can resubmit new information or contact the CBP INFO Center online or by calling 1-877-CBP-5511 to determine how to update their submission. Upon arrival at a POE, the CBP officer can update or edit any inaccurate information that was submitted through CBP One™. Additionally, individuals seeking notification of and access to information contained in CBP holdings, or seeking further information related to their secondary inspection, may gain access to certain information by filing a Freedom of Information Act (FOIA) request with CBP at https://foiaonline.gov/, or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229
Fax Number: (202) 325-1476

U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act request to access their information.

All Privacy Act and Freedom of Information Act requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Requests for information are evaluated by CBP to ensure that the release of information is lawful; will not impede an investigation of an actual or potential criminal, civil, or regulatory violation; and will not reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

7.2 What procedures are in place to allow the subject individual to

correct inaccurate or erroneous information?

Individuals may correct inaccurate or erroneous information directly with the processing CBPO, who will correct the CBP records, at the time of encounter and throughout the secondary inspection process. Individuals can inform CBP officers of inaccurate information if CBP officers ask them a question containing inaccurate information and at any time during secondary inspection.

Any individual who believes that CBP's actions are the result of incorrect or inaccurate information may request information about his or her records pursuant to procedures provided by the Freedom of Information Act. U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act who believe that CBP's actions are the result of incorrect or inaccurate information may request correction of that data under the amendment provisions of the Privacy Act of 1974 by writing to the above address. The CBP Privacy Division reviews all requests for correction and amendment regardless of status.

Travelers may also contact the DHS Traveler Redress Inquiry Program (TRIP) at 601 South 12th Street, TSA-901, Arlington, VA, 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible to identify the record(s) at issue.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures for correcting their CBP information through the System of Records Notices describing each of the underlying systems from which USEC accesses information. This Privacy Impact Assessment also serves as notification. Additionally, signage and tear sheets at POEs provide information on how to contact the DHS Traveler Redress Inquiry Program. In addition, travelers may request information from the on-site CBP officer.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that travelers will not know how to request redress.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment provides information on how to request access and amendments to information within CBP holdings. Additionally, CBP officers located at POEs inform travelers verbally and through tear sheets on how they can challenge a determination and request access to the information that CBP used to make a determination. Travelers who wish to access information about themselves or challenge a determination can submit a Freedom of Information Act request to CBP or a DHS Traveler Redress Inquiry Program request to the addresses above. Additionally, U.S. citizens, lawful permanent residents, and individuals covered by the Judicial Redress Act, may submit a Privacy Act Amendment request to CBP.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CBP implements role-based access for all CBP systems, and only grants access to users who have a demonstrated need to know. All CBP systems secure its data by complying with the requirements of DHS information technology security policy, particularly the DHS Sensitive Systems Policy Directive 4300A.[51] This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. CBP periodically evaluates these systems to ensure that it complies with these security requirements. Each system provides audit trail capabilities to monitor, log, and analyze system transactions as well as actions and system accesses of authorized users. CBP periodically conducts reviews for compliance within the program and between external partners to ensure that the information is used in accordance with the stated acceptable uses documented in the Memoranda of Understanding/Agreement, System of Record Notice, sharing agreements, and other technical and business documentation

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

CBP does not grant access to users of CBP systems without completion of the CBP Security and Privacy Awareness course, which is required to be completed on an annual basis. This course presents Privacy Act responsibilities and agency policy regarding the security, sharing, and safeguarding of both official information and personally identifiable information. The course also provides information regarding sharing, access, and other privacy controls. CBP updates this training regularly, and CBP system users are required to take the course annually.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

System access is based on a demonstrated need to know by a user, and access is only granted with supervisory approval and upon completion of the required security checks. However, the purpose and use of a user's access varies by system. For example, CBP employee access to the CBP One™ system is limited to users from CBP's Office of Information Technology (OIT) in order to perform application updates and correct any issues. TVS assigns non-privileged accounts

[51] *See* DHS 4300A SENSITIVE SYSTEMS HANDBOOK, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

to end users and privileged accounts to account managers or administrators in order to manage and maintain TVS. The TVS system owner determines the conditions for role membership and designates selected individuals to serve as account managers for the system. Once a user successfully completes the application for a TVS account, their supervisor identifies which TVS system role(s) are needed to accomplish the job, and the account manager determines account access. USEC is primarily accessed by CBPOs located at a POE. USEC has provisions and roles to determine what access is provided to users. USEC users have to be separately provisioned to access the source systems that feed into Unified Secondary in order to view that information documented in USEC. Lastly, the advance arrival information that is stored in the segregated ATS database is only accessible by a limited number of CBP employees. However, once the information becomes part of an immigration event or a UPAX event is created, it may be accessed by internal and external partners who have access to ATS. Each user group's access to information in ATS is defined by the specific profile created for that group. Group profiles are intended to limit access by reference to the common need to know and mission responsibilities of users within the group. Access by Users, Managers, System Administrators, Developers, and others to the ATS data is defined in the same manner and employs profiles to tailor access to mission or operational functions.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any information sharing agreements for this data will define the nature of access, the scope of information subject to the sharing agreement, and the privacy, security, safeguarding, and other requirements. All information sharing arrangements are reviewed by the CBP Privacy Officer and the CBP Office of Chief Counsel in accordance with existing CBP and DHS policy.

Contact Official

Matthew Davies
Executive Director
Admissibility and Passenger Programs
Office of Field Operations
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office

U.S. Customs and Border Protection
privacy.cbp@cbp.dhs.gov

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717