Privacy Impact Assessment

for the

Advance Travel Authorization

DHS Reference No. DHS/CBP/PIA-073

October 17, 2022

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) is developing a new, voluntary Advance Travel Authorization (ATA) process to collect information from eligible noncitizens requesting advance authorization to travel to the United States to seek a discretionary grant of parole. U.S. Customs and Border Protection (CBP) is publishing this new Privacy Impact Assessment (PIA) to provide notice and assess the privacy risks associated with ATA. ATA launched October 12, 2022, to implement a parole process for certain undocumented noncitizens from select countries and their qualifying immediate family members, under which those individuals may request advance authorization to travel to the United States to seek a discretionary grant of parole. This Privacy Impact Assessment discusses the general workflow of ATA and the information collected, stored, and used at each step. CBP's ATA collection is conducted through the CBP One™ mobile application, and CBP is publishing a CBP One™ Privacy Impact Assessment appendix update concurrently with this ATA Privacy Impact Assessment.

Overview

On October 12, 2022, Secretary of Homeland Security Mayorkas announced the creation of a new parole process for certain undocumented noncitizens from select countries. Under this process, certain undocumented noncitizens from select countries (as identified in the Appendix to this Privacy Impact Assessment) and their qualifying immediate family members, who are outside of the United States and who lack visas or other appropriate entry documents, may utilize ATA to request an advance authorization to travel to the United States to seek a discretionary grant of parole. Parole allows an individual who may be inadmissible to the United States to be in the United States for a temporary period for urgent humanitarian reasons or significant public benefit.

Generally, a citizen of a foreign country who wishes to enter the United States must first obtain a valid travel authorization. Travel authorizations are typically issued as a visa by the U.S. Department of State, or as an Electronic System for Travel Authorization (ESTA) for citizens of a country that participates in the Visa Waiver Program (VWP).[1] A travel authorization allows a foreign citizen to travel to a U.S. port of entry and apply for admission to the United States. A travel authorization does not guarantee entry into the United States. CBP officials at the port of entry have authority to determine every individual's admissibility to the United States. Regardless of whether a traveler is issued a visa, an Electronic System for Travel Authorization, or ATA, a CBP official will still determine admissibility during inspection at the port of entry.

The Immigration and Nationality Act (INA) allows DHS to exercise discretionary authority to parole a non-U.S. citizen into the United States, on a case-by-case basis, temporarily for urgent

[1] The Visa Waiver Program allows foreign nationals from certain countries to travel to the United States for business or pleasure, for stays of 90 days or less without obtaining a visa.

humanitarian reasons or significant public benefit.[2] DHS has delegated parole authority to CBP, as well as U.S. Immigration and Customs Enforcement (ICE) and U.S. Citizenship and Immigration Services (USCIS).[3] Parole allows an individual who may not have a valid entry document (such as a visa or an Electronic System for Travel Authorization) into the United States for a temporary period.[4]

Absent national security or public safety concerns, individuals arriving with an approved advance authorization to travel to the United States to seek a discretionary grant of parole may be considered for parole; however, inspecting CBP officers retain the discretion to process arriving individuals on a case-by-case basis considering the totality of the circumstances. Using its delegated authority to grant parole, CBP will determine, in an exercise of discretion, whether parole is appropriate at the time that the individual presents themselves for inspection at a U.S. port of entry. The inspecting CBP officer considers the totality of the circumstances when making disposition determinations.

Advance Travel Authorization Process

The new, voluntary ATA process is available to certain undocumented noncitizens from select countries, and their qualifying immediate family members, who are outside of the United States and who lack visas or other entry documents. Appendix A of this Privacy Impact Assessment contains a current list of the ATA eligible countries. ATA eligible noncitizens (referred to throughout the rest of this Privacy Impact Assessment as "travelers") will follow the ATA process, and if approved, will receive an advance authorization that will permit them to travel to the United States to seek parole. If the ATA is denied, the individual will not be authorized to travel to the United States under this process but may pursue other existing avenues to obtain valid United States entry documents such as a visa. The ATA process consists of multiple steps with data capture, verification, and vetting conducted by both USCIS and CBP, in collaboration with the National Vetting Center (NVC). The public facing systems used in the ATA process are USCIS's myUSCIS and CBP's CBP One™ mobile application. Additionally, CBP conducts traveler vetting through the Automated Targeting System (ATS) and other systems, while CBP's Advance Travel Information System (ATIS) is responsible for storing and moving the data.[5]

---

[2] *See* 8 U.S.C. § 1182(d)(5); 8 C.F.R. § 212.5.
[3] *See* DHS Delegation Orders: Delegation of Authority to the Commissioner of U.S. Customs and Border Protection; Delegation No. 7010.3, Sec. 2(B)(15).
[4] An individual who is paroled into the United States has not been admitted into the United States for purposes of immigration law.
[5] *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.

1. myUSCIS

To initiate the process of requesting an advance travel authorization, a U.S.-based supporter electronically files USCIS Form I-134,[6] Declaration of Financial Support, on behalf of the traveler and/or traveler family members. Using this form, USCIS collects personally identifiable information on (1) the U.S.-based supporter, (2) the traveler;[7] (3) an interpreter (if any); and (4) the preparer of the form (if different than the supporter). USCIS uses the information on this form to conduct vetting on the supporter and determines whether the supporter has established a basis of support for the traveler(s).

Following approval of the I-134, USCIS will assign each traveler an A-Number—if they do not already have an assigned A-Number—and will notify the traveler electronically with an invitation to create a myUSCIS account. myUSCIS is a USCIS-owned digital environment where individuals create a secure account to use various digital services and access pending case information.[8] Travelers use their myUSCIS account to verify their biographic information as collected on the Form I-134 is accurate and attest to all requirements. Once the traveler has confirmed their biographic information, myUSCIS informs them to use the CBP One™ mobile application to continue the process.

USCIS sends the I-134 and A-Number with supporting biographic data to CBP, which CBP stores in the Arrival and Departure Information System (ADIS).[9] CBP One™ (described below) validates the traveler's data including their A-Number and passport number against USCIS-provided data stored in the Arrival and Departure Information System and sends this information to CBP's Advanced Traveler Information System. CBP creates a pending ATA and sends the traveler's ATA process data to CBP's Automated Targeting System/Unified Passenger system (UPAX) and the National Vetting Center for ATA vetting. Based on vetting results, CBP's Pre-departure Service[10] provides an ATA status (approved or not approved) to the airlines (if an individual travels by air). CBP also sends ATA status to USCIS to update the traveler's myUSCIS account submission status (Travel Authorized or Travel Not Authorized). Travelers authorized to travel may book commercial airline travel to a U.S. port of entry.

---

[6] *See* Form I-134 Declaration of Financial Support, *available at* https://www.uscis.gov/i-134.
[7] A separate Form I-134 is required for each traveler and eligible family members.
[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE myUSCIS Account Experience, DHS/USCIS/PIA-071, *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM, DHS/CBP/PIA-024, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

2. CBP One™

Once the affidavit of support and associated requirements are complete, USCIS will inform the traveler to complete their request for advance authorization to travel by downloading the CBP One™ mobile application. Once the CBP One™ mobile application is downloaded, the user must select "Traveler," then "Air," then "Advance Travel Authorization," then "Request Advance Travel Authorization." The first time a traveler accesses CBP One™, they will be prompted to provide their first and last name in their profile. After the traveler's name is collected, the traveler will then be directed to manually enter their myUSCIS-provided A-Number.

CBP One™ will then direct the user to "Scan Passport." The CBP One™ mobile application will then display a pop-up notifying the user that the mobile application is accessing the mobile device's camera. Once the camera is enabled, the mobile application prompts the user to position the mobile device's camera over the passport's biographic page. Once the biographic page of the passport is scanned, CBP One™ will determine whether there is a readable eChip[11] imbedded in the passport. If there is a readable eChip, CBP One™ will decode the chip and retrieve the photograph, date of birth, and travel document number associated with the passport. If there is no useable eChip, CBP One™ will collect the photograph on the biographic page and scan the Machine-Readable Zone (MRZ) of the passport to collect the date of birth and passport number, nationality. This biographic information is then automatically populated into the submission of the mobile application to eliminate the need for manual input by the traveler.

In addition to the collection of the biographic information, users who have eChips will be prompted to place their mobile device near the passport's eChip. By placing the mobile device near the eChip, the mobile device enables the Near Field Communication[12] capability to wirelessly retrieve the biometric data stored within the eChip. The biometric information on the eChip includes the passport photograph and country signing certificate to certify the authenticity of the passport.

Once the biographic and eChip data is collected, CBP One™ prompts the user to take a live photograph or "selfie." CBP One™ instructs the user to line their face up with a circle on the screen of their mobile device. CBP One's™ imbedded software then performs a "liveness" test to

[11] An e-Passport contains an electronic chip. The chip holds the same information that is printed on the passport's data page: the holder's name, date of birth, and other biographic information. An e-Passport also contains a biometric identifier. The United States requires that the chip contain a digital photograph of the holder. All e-Passports issued by Visa Waiver Program countries and the United States have security features to prevent the unauthorized reading or "skimming" of data stored on the e-Passport chip. *See* https://www.dhs.gov/e-passports.
[12] Near Field Communication describes a technology which can be used for contactless exchange of data over short distances. Two Near Field Communication-capable devices are connected via a point-to-point contact over a short distance. This connection can be used to exchange data between the devices.

determine that it is real person (and not a picture of a person).[13] CBP One™ allows the user to capture their image and select "Continue" once they satisfied it is an accurate photo. CBP One™ will reject any images that are not correctly captured. If the user is not satisfied with the image captured, the user can retake the image. There is currently no limitation to the number of attempts to retake the selfie to ensure a proper image. If they continue to have technical difficulties, the CBP One™ application provides a help desk email address to provide assistance.

Once the capture of the live photo is verified, the CBP One™ application will display a summary page with all information collected and allow the user to return to previous pages to modify their submission to correct anything that may have been collected incorrectly. Once the user verifies and submits their information, the data and photographs are passed to downstream systems described below. The CBP One™ application will advise the user to refer to their myUSCIS account for further information on their request.

CBP One™ collects and sends the A-Number, date of birth, and passport number to the CBP Arrival and Departure Information System in order to verify the traveler accessing the specific functionality within CBP One™ has a USCIS-approved U.S.-based supporter, has verified their biographic information, and has provided the DHS required attestations related to program eligibility criteria.[14] The Arrival and Departure Information System directly interfaces with USCIS's Electronic Immigration System (ELIS), which is used to process immigration benefits.[15] If the Arrival and Departure Information System confirms the information to be valid, a confirmation will be sent back to CBP One™, and then CBP One™ will send the biographic information, A-number, and passport number to the Automated Traveler Information System for vetting.[16] CBP uses the passport number to conduct document verification in TECS, the primary system used by CBP officers at the border to assist with screening and admissibility, to determine if the document is valid.[17] If CBP cannot confirm that the traveler has been approved by USCIS

[13] While the user is taking the selfie, the technology embedded within the mobile application relies on the device's camera to view a live image through 3D face changes and observing perspective distortion to prove the image is 3D. If "liveness" cannot be confirmed, the user is unable to utilize the CBP One™ application.
[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024, *available at* https://www.dhs.gov/privacy-impact-assessments.
[15] *See* DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES (USCIS), PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC IMMIGRATION SYSTEM (USCIS ELIS), DHS/USCIS/PIA-056, *available at* https://www.dhs.gov/privacy, and DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016).
[16] The Advanced Traveler Information System is a web-based application and screening system used to vet undocumented noncitizens applying for advance authorization to travel to the United States and seeking parole.
[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates), and U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE

for ATA or identify a valid passport the traveler will not be able to complete their request for advance authorization to travel.

Once all the required information and photograph are submitted, the information is saved in the Advanced Traveler Information System and copied to Automated Targeting System- Unified Passenger system for biographic and biometric (photograph) vetting. CBP does not search or enroll photographs submitted via the CBP One™ mobile application to the Automated Biometric Identification System/Homeland Advanced Recognition Technology System (IDENT/HART).[18] CBP One™ informs the traveler that CBP has received the information and it is being reviewed and reminds the traveler to check their myUSCIS account for any updates. In addition to this Privacy Impact Assessment, CBP has completed an appendix update to the CBP One™ Privacy Impact Assessment which provides full detail on the data collection process in CBP One™ for ATA travelers.

Uses of Facial Comparison During ATA Process

CBP uses facial comparison technology at various stages in the ATA process. After CBP One™ captures the photograph, it first sends that image to the Advanced Traveler Information System where CBP uses it for several different purposes.

CBP uses the selfie image for five distinct purposes: (1) to conduct one-to-one (1:1) facial comparison against the passport photograph previously uploaded to the ATA CBP One™ function from the eChip; (2) to conduct one-to-many (1:n) vetting against derogatory photographic holdings for law enforcement and national security concerns as part of the ATA vetting process; (3) to generate a new gallery of ATA participants for facial comparison when ATA participants arrive at a port of entry; (4) to conduct 1:n identity verification once the participants arrive at the port of entry; and (5) to conduct 1:n vetting against known derogatory photographs for assistance in CBP's admissibility determination.

TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-impact-assessments.

[18] *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/privacydocuments-office-biometric-identity-management-obim. DHS is in the process of replacing the Automated Biometric Identification System with the Homeland Advanced Recognition Technology System as the primary DHS system for storage and processing of biometric and associated biographic information. For more information about the Homeland Advanced Recognition Technology System, 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 a*t https://www.dhs.gov/privacydocuments-office-biometric-identity-management-obim.

Using the Traveler Verification Service (TVS)[19] functionality within the Automated Targeting System-Unified Passenger system, CBP compares the two photographs to conduct a 1:1 match with the selfie and the user's passport photograph to biometrically verify the user's identity. If the two photographs are a match, Automated Targeting System-Unified Passenger system will send a match response back to CBP One™. CBP One™ allows the user to capture their image and confirm submission after viewing the captured image. CBP One™ will only allow submission of an image of sufficient quality. If the image is not of sufficient quality or the user is otherwise not satisfied with the image captured, the user can retake the image until a quality image is captured. There is currently no limitation to the number of attempts to retake the selfie to ensure a proper image. If the individual continues to have technical difficulties, the CBP One™ application provides a help desk email address to provide assistance.

Once the 1:1 biometric verification is complete, the CBP One™ application will display a summary page with all information collected and allow the user to edit anything that may have been collected incorrectly. Once the user verifies and submits their information, the vetting process begins, and the mobile application will advise the user to refer to their myUSCIS account for further information on their request.

When all the required information and photograph are submitted, the information is saved in the Advanced Traveler Information System and copied to Automated Targeting System-Unified Passenger system for biographic and biometric (photograph) vetting. CBP does not search or enroll photographs submitted via the CBP One™ mobile application to the IDENT/HART[20] system. CBP One™ informs the traveler that CBP has received the information and it is being reviewed and reminds the traveler to check their myUSCIS account for any updates. In addition to this Privacy Impact Assessment, CBP has completed an appendix update to the CBP One™ Privacy Impact Assessment which provides full detail on the data collection process in CBP One™ for ATA travelers.

3. Advance Travel Information System

CBP stores information collected from travelers via CBP One™ in CBP's Advance Travel Information System. The Advanced Traveler Information System is a storage system used by CBP to automatically coordinate vetting by sending information collected via CBP One™ and USCIS to the vetting systems and receiving a consolidated response. Upon receipt, the Advanced Traveler

[19] 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 recognition, 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 (2018), *available at* https://www.dhs.gov/privacydocuments-us-customs-and-border-protection.

Information System provides traveler ATA data to CBP's Automated Targeting System[21] where it is vetted against selected DHS and other federal agency security and law enforcement databases for national security, border security, public health, and safety concerns. In addition, the Automated Targeting System will share that biographic data with the National Vetting Center for classified vetting support.[22] CBP conducts this vetting to determine whether the beneficiary poses a security risk to the United States and whether they may be eligible to obtain advance authorization to travel to the United States to seek a discretionary grant of parole. The results of this vetting help to inform CBP's assessment of whether the beneficiary's travel poses a law enforcement or security risk and whether the request should be approved. CBP consolidates both the unclassified and classified vetting results in the Advanced Traveler Information System and sends an approval or denial message to USCIS.

If the ATA submission is denied, the beneficiary is not eligible to receive an advance authorization to travel to the United States to seek a discretionary grant of parole under this process. CBP retains all ATA denials in the same manner as Electronic System for Travel Authorization denials, where they are treated as a law enforcement record and stored for 75 years. If the submission is approved, the approval establishes that the beneficiary has obtained advance authorization to travel to the United States to seek parole but does not guarantee boarding or a specific processing disposition. Upon arrival at a U.S. port of entry, the traveler will be subject to inspection by a CBP officer, who will make a case-by-case processing disposition determination.

4. Entry and Processing

Upon arrival at a U.S. port of entry, travelers will undergo inspection and examination in the same manner as any other traveler. If traveling by commercial air to the United States under the ATA process, individuals must show their ATA submission status along with a valid passport and other appropriate identification to airline personnel. Air carriers that participate in CBP's Document Validation program[23] can validate an approved and valid travel authorization submission using the same mechanisms that are currently in place to validate that a traveler has a valid visa or other documentation to facilitate issuance of a boarding pass for air travel. Carriers not participating in CBP's Document Validation program may request verification of the traveler's Travel Authorization status by viewing the individual's myUSCIS account and should contact the Regional Carrier Liaison Group (RCLG) if additional confirmation of the travel authorization status is warranted.

---

[22] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE NATIONAL VETTING CENTER, DHS/ALL/PIA-072, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[23] *See* CBP Carrier Liaison Program for more information *available at* https://www.cbp.gov/travel/travel-industry-personnel/carrier-liaison-prog.

All individuals are subject to inspection by a CBP officer upon arrival at a U.S. port of entry.[24] Although the population utilizing this process will be arriving at the port of entry with an approved ATA submission, they will not be in possession of valid United States entry documents. Therefore, consistent with current policy, these individuals will be referred for secondary inspection. The Unified Secondary system (USEC)[25] will display an individual's travel authorization submission and travel authorization status as part of the system checks conducted during inspection to allow the inspecting officer to determine the appropriate processing disposition.

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?

Pursuant to 8 U.S.C. § 1182(d)(5), CBP has the authority and discretion to grant parole to noncitizens, as appropriate, on a case-by-case basis, for urgent humanitarian reasons or significant public benefit.[26] Pursuant to 8 C.F.R. § 212.5(f), DHS may issue an "appropriate document authorizing travel" to a noncitizen without a visa who is traveling to the United States to seek parole.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The Automated Targeting System (ATS) System of Records Notice (SORN)[27] covers the

[24] See 8 C.F.R. Part 235 Inspection of Persons Applying for Admission. If an individual arrives at a port of entry without sufficient documentation, as part of standard processing the CBP officer typically refers the individual for a secondary inspection. For a full description of the privacy risks and mitigations associated with CBP primary and secondary processing procedures, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates); TECS SYSTEM PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[25] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR UNIFIED SECONDARY, DHS/CBP/PIA-067 (2021 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[26] Parole allows a noncitizen to temporarily enter the United States where such parole provides a significant public benefit or is for an urgent humanitarian reason. The Immigration and Nationality Act (INA) allows authorized DHS officials to use their discretion to parole any noncitizen applying for admission into the United States for urgent humanitarian reasons or significant public benefit (See 8 U.S.C. § 1282(d)(5); 8 C.F.R. § 212.5). An individual who is paroled into the United States has not been admitted into the United States for purposes of immigration law.

[27] *See* DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

collection of information from persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States by land, air, or sea, or through other locations where CBP maintains an enforcement or operational presence. Information from travelers requesting advance authorization to travel to the United States to seek parole is broadly covered by the Automated Targeting System System of Records Notice. CBP compares the advance information against law enforcement and intelligence databases, which allows CBP to identify individuals and cargo requiring additional scrutiny, which aligns to the border security mission of the Department.

The Alien File, Index, and National File Tracking System of Records Notice[28] covers the A-number and information regarding transactions involving an individual as they pass through the U.S. immigration process. The Benefit Information System (BIS) System of Records Notice[29] covers information contained in myUSCIS.

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

The user's biographic data, passport number, and citizenship data submitted through the CBP One™ application is stored in an Amazon Web Services cloud for 365 days for purposes of reporting aggregate data for CBP leadership. CBP One™ will not store any photographs. CBP One™ also collects the first and last name of the user as part of the profile creation and this information is stored locally on the user's device to create a user profile within CBP One™ so that the user can quickly retrieve information for subsequent use.

Advanced Traveler Information System data resides within the e-Business Cloud security boundary. The e-Business Cloud Authority to Operate (ATO) was last renewed in June 2022.

Advanced Traveler Information System information is also transferred and stored in the Automated Targeting System, for 15 years. The Automated Targeting System underwent the security authorization process in accordance with DHS and CBP policy, which complies with federal statutes, policies, and guidelines. The Automated Targeting System received a renewed Authority to Operate on January 15, 2020.

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

[28] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (September 18, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.
[29] *See* DHS/USCIS-007 Benefit Information System (BIS) System of Records, 84 FR 54622 (October 10, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.

No. CBP is in the process of developing formal records retention schedule(s) for ATA and other traveler encounter records. However, the various types of data collected by the ATA process have various proposed records schedules:

1. CBP stores the Form I-134 basic biographic information submitted by supporters within the Arrival and Departure Information System consistent with its retention schedule of 75 years, and consistent with other information received from USCIS on various immigration forms.
2. The Arrival and Departure Information System then passes the basic biographic information to the Advanced Traveler Information System where it is combined with the user-submitted data from CBP One™ and stored for 15 years, consistent with the Electronic System for Travel Authorization retention schedule (another advance travel authorization program).
3. CBP also stores a copy of this information within the Automated Targeting System as a copy from the Advanced Traveler Information System for faster vetting. While most Automated Targeting System records are retained for 15 years, records that are of law enforcement interest, such as an ATA denial, are stored consistent with other law enforcement encounters for 75 years.
4. CBP One™ is a passthrough for information and does not store any official biographic or biometric record. The user's biographic data, passport number, and citizenship data submitted through the CBP One™ application is stored in a CBP-owned cloud storage solution for 365 days for auditing purposes and reporting aggregate data.
5. For the selfie photograph used only for identity verification against the traveler's passport photograph, CBP will store this photograph in the Automated Targeting System and the Advanced Traveler Information System for the duration of the validity of the travel authorization (generally 90 days unless granted an extension), or traveler passport expiration date (whichever is sooner).
6. For photographs collected as part of the entry process at the port of entry, these records are stored for 75 years consistent with the DHS Office of Biometric Information Management (OBIM) current Record Schedule DAA-0563-2013-0001. This schedule covers DHS biometric and biographic records used for national security, law enforcement, immigration, and other functions.

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 is concurrently seeking a new emergency approval from the Office of Management and Budget (OMB) under the Paperwork Reduction Act to permit this collection.

Section 2.0 Characterization of the Information

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

CBP receives the information listed below from USCIS, submitted by the supporter about the traveler(s) via the Form I-134, and stores it in the Arrival and Departure Information System, Advanced Traveler Information System, and Automated Targeting System-Unified Passenger system:

- Full name (first, middle, last)
- Date of birth
- Gender
- Receipt number
- Form type
- Case status
- Event date
- A-Number
- Country of citizenship
- Country of birth
- Country of residence
- Passport number
- Document country of issuance
- Passport issue date
- Passport expiration date
- Physical address (street, city, state, country, zip code)
- Telephone number (home, mobile, other)
- Email address
- Birthplace (city, state, country)

- USCIS ELIS account number

In addition to the data passed to CBP from USCIS, CBP collects information directly from the traveler via CBP One™. When prompted by USCIS to create an account and continue to the advance travel authorization process, the traveler logs into CBP One™ using a Login.gov account and enters their A-Number. CBP One™ validates the traveler's A-Number against the A-Number stored in the Arrival and Departure Information System. The traveler scans their passport using embedded Machine-Readable Zone scan technology in CBP One™ which auto-captures the passport number, date of birth and citizenship, as well as a photograph either via eChip in ePassports or directly from the passport's biographic page. Finally, CBP One™ collects a live photograph or selfie.

CBP creates the full Advanced Traveler Information System record using the traveler's A-Number, passport number, date of birth, travel document photograph and selfie from CBP One™, and from the Form I-134 biographic information submitted from USCIS via CBP's Arrival and Departure Information System.

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

For the ATA process, USCIS and CBP collect this information directly from the individuals applying as U.S.-based supporters, and from the individual(s) seeking to obtain advance authorization to travel to the United States.

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

Yes. CBP may vet submissions against commercial sources and/or publicly available data, including social media information, through its established vetting procedures. This information provides supplemental data about persons or businesses as part of the analysis process for researching individuals requiring additional vetting.

2.4 Discuss how accuracy of the data is ensured.

CBP collects this information directly from the supporter seeking to obtain advance authorization to travel for certain eligible noncitizens (via myUSCIS), and from the travelers themselves. While there is always an inherent risk to manual data entry, CBP provides individuals with the opportunity to review and verify the information prior to submission to CBP. Additionally, once an individual presents him or herself for inspection upon arrival at a port of entry, a CBP officer verifies and updates any information in inspection systems that is incorrect or inaccurate.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that individuals will be denied an ATA if the facial recognition tools determine a "no match" between the new selfie and an individual's travel document.

Mitigation: This risk is mitigated. CBP One™ allows the user to capture their image and confirm submission after viewing the captured image. If the user is not satisfied with the image captured, the user can retake the image. There is currently no limitation to the number of attempts to retake the selfie to ensure a proper image. If they continue to have technical difficulties, the CBP One™ application provides a help desk email address to provide assistance. CBP One™ will only allow submission of an image of sufficient quality.

There are two types of facial comparison used for ATA. The first is a 1:1 match for identity verification against an individual's travel document photograph and a new, live selfie as part of the CBP One™ process. This 1:1 match has a very high match accuracy rate since the match is one photograph to another one photograph.

The second is a 1:n match using the newly submitted ATA selfie photograph against other CBP holdings of derogatory photographs. A match against a known derogatory photograph does not automatically trigger an ATA denial; rather, the entire ATA submission will be manually reviewed by a CBP officer to determine whether the match is accurate and whether the ATA should be denied.

Privacy Risk: There is a risk of overcollection since CBP may collect information from individuals who do not actually arrive at the port of entry.

Mitigation: This risk is partially mitigated. CBP is collecting this information from individuals who are seeking to obtain advance authorization to travel to the United States to seek parole. Individuals voluntarily provide this information to CBP. This information collection is similar to other advance information collections, such as Advance Passenger Information System (APIS)[30] data and Electronic System for Travel Authorization [31] data. In this circumstance, CBP also collects and retains information on individuals who may intend to travel but do not actually travel to the United States. This advance information, combined with the results of the pre-vetting,

[30] *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.
[31] *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.

is used by CBP to identify public safety threats (such as wants/warrants) and national security threats (such as links to terrorist organizations).

Privacy Risk: There is a risk that information submitted to CBP will be inaccurate.

Mitigation: This risk is mitigated. Though supporters submit the initial biographic information about travelers, all travelers are granted access to myUSCIS, where they can verify their biographic information as collected on the Form I-134 is accurate and attest to all requirements. Once the traveler has confirmed their biographic information, myUSCIS informs them to use the CBP One™ mobile application to continue the process.

All information that CBP collects through CBP One™ is done automatically through either a scan of the Machine-Readable Zone on the passport or decoding the eChip embedded in the passport. Absent fraud, CBP can rely on this information being accurate. If the information submitted through CBP One™ does not match the information in the approved Form I-134, the user is advised to return to their myUSCIS account and verify the information is accurate and matches the submission in CBP One™.

Privacy Risk: There is a risk that CBP is collecting more information than necessary to issue a travel authorization.

Mitigation: This risk is mitigated. CBP is collecting the same biographic information that is typically collected from individuals seeking to travel to the United States (*e.g.*, Advance Passenger Information System, Electronic System for Travel Authorization, Form I-94, *Arrival/Departure Record,* or Form I-94W, *Nonimmigrant Visa Waiver Arrival/Departure Record),*[32] and the same biographic and biometric information as part of a U.S. Department of State visa application. Additionally, the information collected in advance of an individual's arrival is consistent with the information that CBP normally collects at the port of entry during the inspection in accordance with existing CBP processes.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP uses the information from the ATA submission to grant or deny advance authorization for an individual to travel to the United States to seek parole. CBP also uses the information to determine whether the individual seeking advance authorization to travel poses a law enforcement or security risk to the United States.[33] CBP vets the information against selected security and law enforcement databases at DHS, including TECS and the Automated Targeting System, as well as

[32] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE I-94 WEBSITE SUBMISSION, DHS/CBP/PIA-016 (2013 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[33] See 8 U.S.C. § 1187(h)(3).

leveraging the National Vetting Center process. CBP may use tools and search techniques to locate publicly available information, including social media information, about the individual seeking advance authorization to travel.[34]

Pre-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 pre-vet to pre-determine a particular processing disposition or an individual's admissibility to the United States. CBP officers determine an individual's processing disposition and, as appropriate, admissibility, on a case-by-case basis and consider the totality of the facts and circumstances known to the CBP officer at the time of inspection. CBP officers do not make any disposition determinations in advance of an encounter with an individual.

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.

No. ATA does not analyze any data for predictive patterns, but rather conducts name matching and screening using existing DHS systems. ATA information stored within the Automated Targeting System 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?

Yes. While the advance information stored in the Advanced Traveler Information System is typically not available for access by other DHS components, all ATA information is sent to the Automated Targeting System and may be accessed by DHS components who have appropriate access provisions within Automated Targeting System entitlements. Furthermore, information that is input into Unified Secondary upon the individual's arrival at a port of entry may be accessed by other components with proper entitlements. While the roles and responsibilities in Unified Secondary 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

[34] The use of publicly available information on social media platforms to grant or deny an advance authorization complies with DHS Management Directive 110-01-011 "Privacy Policy for Operational Use of Social Media," and was approved by the DHS Privacy Office for certain offices within CBP.

Enforcement Integrated Database (EID) as immigration events.[35] Additionally, biometric and associated biographic information collected during the inspection process may be searched and enrolled in the Automated Biometric Identification System/Homeland Advanced Recognition Technology System.[36]

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that CBP will conduct pre-arrival vetting checks on individuals who do not arrive at a U.S. port of entry.

Mitigation: This risk is partially mitigated. CBP may conduct pre-arrival vetting on individuals who never arrive in the United States since this use is consistent with current CBP operations, such as when CBP receives advance passenger information (API) 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).

Privacy Risk: There is a risk that CBP will use the selfie collected by CBP One™ for purposes beyond identity verification and vetting for ATA determination.

Mitigation: This risk is mitigated. CBP will use the selfie photograph for five purposes:(1) to conduct one-to-one (1:1) facial comparison against the passport photograph previously uploaded to the ATA mobile application from the eChip; (2) to conduct (1:n) vetting against derogatory photographic holdings for law enforcement and national security concerns as part of the ATA vetting process; (3) to generate a new gallery of ATA participants for facial comparison when

[35] The Enforcement Integrated Database is a DHS shared common database repository used by several DHS law enforcement and homeland security applications. Enforcement Integrated Database 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, USCIS, and CBP. Enforcement Integrated Database 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/privacy-documents-ice.

[36] *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. DHS is in the process of replacing the Automated Biometric Identification System with the Homeland Advanced Recognition Technology System as the primary DHS system for storage and processing of biometric and associated biographic information. For more information about the Homeland Advanced Recognition Technology System, 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 a*t https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

ATA participants arrive at a port of entry; (4) to conduct (1:n) identity verification once the participants arrive at the port of entry; and (5) conduct (1:n) vetting against known derogatory photographs for admissibility determination. For the selfie photograph used only for identity verification against the traveler's passport photograph, CBP will store this photograph in the Automated Targeting System and Advanced Traveler Information System for the duration of the validity of the travel authorization (generally 90 days unless granted an extension), or traveler passport expiration date (whichever is sooner). If the photograph is a match against national security or law enforcement derogatory information, the photograph will be saved consistent with other law enforcement encounters for 75 years.

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.

Individuals are provided notice of use of the CBP One™ mobile application and the collection of information described above when the traveler receives the approval notice from myUSCIS that explains next steps. CBP also provides notice to the individual at the time of the electronic collection in the CBP One™ mobile application.

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

Participating in the ATA process is entirely voluntary. Individuals do not have the right to consent to particular uses of the information. Individuals may only choose whether or not they will submit their information as part of this process, in order to request advance authorization to travel to the United States. Once an individual submits their information through CBP One™, they cannot exert control over the use of that data, aside from their ability to amend specific data elements by accessing his or her account and submitting these data elements.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not understand how their information will be used once submitted via CBP One™ to the U.S. Government.

Mitigation: This risk is partially mitigated. All information submitted to CBP via CBP One™ is voluntarily submitted by individuals utilizing the process. CBP provides a Privacy Act Statement at the point of collection on the CBP One™ application and is in the process of publishing a publicly available information collection statement under the Paperwork Reduction Act in the Federal Register. This Privacy Impact Assessment also provides a measure of notice on the use of information collected from the traveler.

Section 5.0 Data Retention by the Project

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

CBP collects and maintains information from various sources as part of the ATA process. CBP stores the Form I-134 basic biographic information submitted by supporters within the Arrival and Departure Information System consistent with its retention schedule of 75 years, and consistent with other information received from USCIS on various immigration forms. The Arrival and Departure Information System then passes the basic biographic information to the Advanced Traveler Information System where it is combined with the user-submitted data from CBP One™ and stored for 15 years, consistent with the Electronic System for Travel Authorization retention schedule (another advance travel authorization program). CBP also stores a copy of this information within the Automated Targeting System as a copy from the Advanced Traveler Information System for faster vetting. Records that are of law enforcement interest, such as an ATA denial, are stored consistent with other law enforcement records for 75 years within the Automated Targeting System Targeting Framework. Justification for a 15- and 75-year retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader experience of the law enforcement and intelligence communities.

CBP One™ is a passthrough of information and does not store any official biographic or biometric record. The user's biographic data, passport number, and citizenship data submitted through the CBP One™ application is stored in a CBP-owned cloud storage solution for 365 days for auditing purposes and reporting aggregate data for CBP leadership. CBP One™ also collects the first and last name of the user as part of the profile creation and this information is stored locally on the user's device to create a user profile within CBP One™ so that the user can quickly retrieve information for subsequent use.

For the selfie photograph used only for identity verification against the traveler's passport photograph, CBP will store this photograph in the Automated Targeting System and Advanced Traveler Information System for the duration of the validity of the travel authorization (generally 90 days unless granted an extension), or traveler passport expiration date (whichever is sooner). Photographs used for vetting to make a travel authorization determination, and new photographs collected as part of the entry process at the port of entry, are stored for 75 years consistent with the DHS Office of Biometric Information Management current record schedule.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk of overcollection since CBP may retain information from USCIS about individuals who do not submit an advance travel authorization via CBP One, or individuals who provide information through the CBP One™ application but do not travel to the United States.

Mitigation: This risk is partially mitigated. Advance travel authorizations are only valid for 90 days (unless granted an extension), or traveler passport expiration date (whichever is sooner), after which CBP will delete selfie photographs used for identity verification. While CBP anticipates that most travelers who are submitted as beneficiaries by a supporter using the ATA process will complete their portion of the ATA process, it is possible that CBP will retain information collected by USCIS about individuals who do not use the ATA process. However, this process is consistent with CBP's storage of other immigration forms from USCIS within the Arrival and Departure Information System to create a person-centric record about an individual's immigration and border security related actions.

Privacy Risk: There is a risk that information will be retained for longer than necessary.

Mitigation: This risk is not yet mitigated. CBP is in the process of developing a records retention schedule for ATA information in the Advanced Traveler Information System. CBP proposes retaining information for 15 years, which is consistent with other advance travel authorizations such as the Electronic System for Travel Authorization. This retention period is based on CBP's historical encounters with suspected terrorists and other criminals, as well as the broader experience of the law enforcement and intelligence communities. If the record is linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases (*i.e.*, specific and credible threats; flights, travelers, and routes of concern; or other defined sets of circumstances), the record will remain accessible for the life of the law enforcement matter to support that activity and other enforcement activities that may become related, and which are retained in TECS.

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.

The information submitted by the individual seeking advance authorization to travel is used for vetting and may be shared, on a need to know basis or pursuant to information sharing arrangements with other agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement or intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. Additionally, CBP may share ATA information consistent with routine uses outlined in the Automated Targeting System System of Records Notice and other Privacy Act conditions for disclosure.

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

Disclosure of ATA data to an agency outside of DHS must be compatible with the purposes for which the data was collected and authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3), specifically the routine uses set forth in the Automated Targeting System System of Records Notice or as otherwise permitted by the Privacy Act.

6.3 Does the project place limitations on re-dissemination?

Information that is disclosed from ATA to another agency may not be disseminated to third parties without the written consent of CBP.

6.4 Describe how the project maintains a record of any disclosures

External sharing is appropriately logged pursuant to subsection (c) of the Privacy Act, which requires the Department to maintain a log of when records have been shared outside of DHS.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the data used for the ATA process and stored in CBP systems such as the Advanced Traveler Information System will be shared under inappropriate circumstances and inconsistent with the original purpose of collection.

Mitigation: This risk is partially mitigated. Absent any legal prohibitions, CBP may share information from the Advanced Traveler Information System with other DHS or component personnel who have an authorized purpose for accessing the information in performance of his or her duties, possess the requisite security clearance, and assure adequate safeguarding and protection of the information. In addition, CBP may share information externally consistent with the Privacy Act and routine uses published in the Automated Targeting System System of Records Notice, and consistent with DHS policy and existing memoranda of understanding (MOU), including setting forth the restrictions on and conditions of use; securing, storing, handling, and safeguarding requirements; and controls on further dissemination.

Privacy Risk: There is a risk that the data shared with an agency on a need-to-know basis or pursuant to an information sharing arrangement may be further shared with a third-party agency.

Mitigation: This risk is partially mitigated. When information is shared with an agency, specific re-dissemination language will be in the information sharing arrangement that limits third-party disclosure without prior authorization from CBP.

Section 7.0 Redress

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

In the event that an individual is not authorized to travel under this process, they may still seek entry through another process, including by filing a request for consideration of parole with USCIS or applying with the Department of State to obtain a visa. Due to the secure nature of the vetting and screening process, CBP cannot offer additional information to individuals about the process or provide details about the status and/or result of a beneficiary's travel authorization review. If travel authorization is denied, CBP is unable disclose information as to why the denial occurred. Individuals with questions regarding the ATA process may contact the DHS Traveler Redress Inquiry Program (TRIP) at https://www.dhs.gov/dhs-trip. For information about CBP's facial comparison program generally, please visit https://biometrics.cbp.gov/ or review the public-facing Privacy Impact Assessment for the Traveler Verification Service.[37]

Individuals seeking notification of and access to information contained in CBP holdings, or seeking further information related to his or her secondary inspection, may gain access to certain information by filing a Freedom of Information Act (FOIA) request with CBP at https://foia.cbp.gov/palMain.aspx, 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 telephone 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?

[37] 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 recognition, 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 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Once arriving at a port of entry, all ATA individuals will be referred for secondary inspection. Individuals may correct inaccurate or erroneous information directly with the processing CBP officer who will correct the information in Unified Secondary, at the time of encounter and throughout the secondary inspection process.

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 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 his or her information?

Individuals are notified of the procedures for correcting their information through the System of Records Notices describing each of the underlying systems from which CBP accesses information. This Privacy Impact Assessment also serves as notification. Additionally, signage and tear sheets at ports of entry provide information on how to contact DHS TRIP. Travelers may also request information from an 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 mitigated. This Privacy Impact Assessment provides information on how to request access and amendments to information within CBP holdings. Additionally, CBP officers located at ports of entry 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 TRIP request to the addresses above. Additionally, U.S. citizens, lawful permanent residents, and individuals who have records covered under 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?

All CBP systems used for the ATA process have role-based access that is granted to users who have a demonstrated need to know. CBP secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS Sensitive Systems Policy Directive 4300A.[38] This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and submission rules. CBP periodically evaluates these systems to ensure that they comply 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 information 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 system access is not activated for any user 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.

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

CBP secures information in compliance with the DHS Sensitive Systems Policy Directive 4300A and corresponding implementation Handbook. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and submission rules. To gain access to CBP systems, a user must not only have a need to know but must also have an appropriate background clearance and completed annual privacy training. A supervisor submits the request to the Office of Information and Technology (OIT) at CBP indicating the individual has a need to know for official purposes. The Office of Information and

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

Technology verifies that the necessary background check and privacy training has been completed prior to issuing a new internal user account. Internal user accounts are reviewed annually to ensure that these standards are maintained. These rules also require a periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of the systems to which they gain access.

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 privacy, security, safeguarding, and other requirements. All CBP information sharing agreements 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
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX A

(Updated January 5, 2023)

Citizens from the following countries determined by the Secretary of the Department of Homeland Security, and their qualified immediate family members, are eligible to participate in the ATA process:

1. Venezuela (eligible on October 12, 2022)
2. Nicaragua (eligible on January 6, 2023)
3. Cuba (eligible on January 6, 2023)
4. Haiti (eligible on January 6, 2023)