Privacy Impact Assessment

for

CBP One™

DHS Reference No. DHS/CBP/PIA-068

February 19, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), launched a new public-facing application, CBP One™, to provide the public a single portal to a variety of CBP services. The application is available on both web and mobile devices. CBP One™ will eventually replace and upgrade existing CBP public-facing mobile applications to improve user interaction and services. CBP One™ includes different functionality for travelers, importers, brokers, carriers, International Organizations, and other entities under a single consolidated log-in and uses guided questions to help users determine the correct services, forms, or applications needed. CBP is conducting this Privacy Impact Assessment (PIA) to address privacy risks in the deployment and use of the CBP One™ mobile application.

Introduction

On October 28, 2020, CBP launched the CBP One™ application. CBP One™ is an application that serves as a single portal to a variety of CBP services. Through a series of guided questions, the application will direct each type of user to the appropriate services based on their needs.

CBP One™ is available for Android and iOS mobile devices in the Google Play or iTunes mobile application stores, as well as on the web at CBP One (dhs.gov). Users must create a new or open an existing Login.Gov[1] account in order to access CBP One™. Login.Gov ensures a secure connection and identity verification for CBP One™ users. To register with Login.gov, users have to provide an email address and a phone number and create a password. Login.gov does not share any information provided by the user with CBP. Each time a user launches CBP One™, a notification displaying the CBP Privacy Policy will appear and users must consent to it prior to using the mobile application.

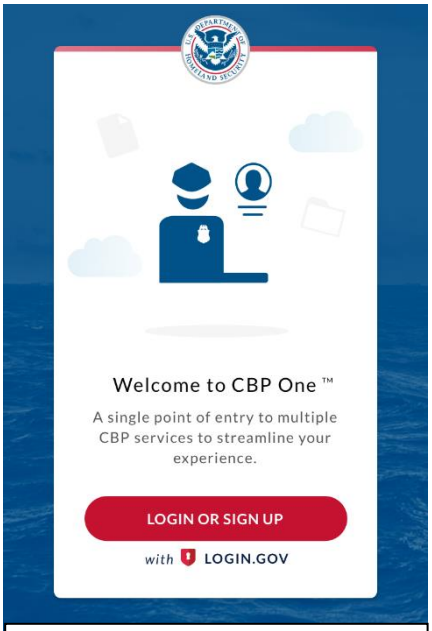


Figure 1: CBP One Login Screen

Once the user has logged in via Login.gov and consented to the privacy policy, the landing page will launch which permits the user to select from different options that describe the individual's reason for using CBP One™. CBP One™ will display different functions based on the user's selections. For some functions, users are able to input

[1] *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.

information for themselves, as well as for others. This makes it easier for groups to submit information, and streamlines CBP's vetting and inspection processes.

Currently, CBP One™ is available for brokers/carriers/forwarders to make appointments for the inspection of perishable cargo and travelers to apply for and view their I-94s. In addition, CBP One™ is available to International Organizations,[2] authorized by persons asserting enrollment in the Migrant Protection Protocols (MPP)[3] Program, to submit biometric and biographic information to verify enrollment in MPP on their behalf.

Eventually, aircraft operators, bus operators, seaplane pilots, commercial truck drivers, vessel operators, or agents will be able to use CBP One™. CBP will add appendices to this PIA to describe new functions as they are launched in the application. Depending on the function, CBP may also publish standalone, function-specific PIAs to fully analyze the risks and mitigations CBP has put in place to protect individual privacy.

Travelers

Individuals traveling into or exiting the United States will be able to use CBP One™ to inform CBP of their arrival and departure consistent with applicable laws. Additionally, travelers will be able to use CBP One™ to apply for certain CBP benefits, such as membership into CBP's Trusted Traveler Program, as well as view some information CBP may maintain on the traveler.

At launch, the I-94 functionality in CBP One™ mirrored the I-94 website functionality.[4] This allows nonimmigrant aliens to apply for a provisional I-94, pay in advance of arrival for an I-94, retrieve their most recent I-94, view their travel history, and check their authorized period of stay on any active I-94. By Summer 2022, CBP will pilot a new Self-Reporting Mobile Exit feature. This new feature will allow some nonimmigrant aliens to self-report their exit from the United States at certain ports of entry on the Northern Border. Appendix A of this PIA describes

[2] An International Organization is an organization that established a treaty or other instrument governed by international law and possessing its own international legal personality, such as the United Nations (UN), the World Health Organization (WHO), and North Atlantic Treaty Organization (NATO). For the purpose of this Privacy Impact Assessment, International Organizations have established roles supporting the Government of Mexico to provide services to undocumented individuals under the Migrant Protections Protocol (MPP).

[3] The Migrant Protection Protocols are a U.S. Government action whereby certain foreign individuals entering or seeking admission to the United States from Mexico – illegally or without proper documentation – may be returned to Mexico and wait outside of the United States for the duration of their immigration proceedings, where Mexico will provide them with all appropriate humanitarian protections for the duration of their stay. Additional information is *available at* https://www.dhs.gov/news/2019/01/24/migrant-protection-protocols. Appendix C of this PIA further outlines the implementation of MPP through CBP One™.

[4] *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.

the I-94 functionality of CBP One™ and CBP will publish a standalone, function-specific PIA before making the Self-Reporting Mobile Exit feature active.

Also, CBP plans on moving the standalone CBP ROAM™ mobile application under the CBP One™ umbrella. CBP ROAM™ permits small pleasure boat operators along the Northern Border to report their arrival into United States. In the future, CBP ROAM™ will be removed from the Google Play and iOS mobile application stores, and travelers will have to use CBP One™ to complete the same transactions. CBP will update Appendix A of this PIA and publish a standalone, function-specific PIA once this offshore arrival reporting functionality is available in CBP One™.

Broker/Carrier/Forwarder Agents

The Inspection Appointment request feature allows brokers/carriers/forwarders to schedule and check the appointment status of an inspection of commercial vessels or for cargo entering the United States. CBP One™ streamlines the scheduling process, which previously required multiple phone calls and exchange of information between brokers/carriers/forwarders and CBP officers or agriculture specialists. Using CBP One™, brokers/carriers/forwarders create a profile that includes contact and port of entry information. Users then request a specific day and time for inspection of their vessel or goods by a CBP officer or agriculture specialist. CBP officers or agriculture specialists use a dashboard outside of CBP One™ to view the requests and assign inspection times. The CBP officer or agriculture specialist can also use the dashboard to communicate with the broker/carrier/forwarder, using CBP One™, in order to gain any additional information. Finally, brokers/carriers/forwarders are able to cancel and reschedule an inspection request through CBP One™. CBP One™ inspections of cargo can also be accessed via a desktop application. In the future, CBP plans to incorporate all cargo into the desktop application.

Operators

Operators are representatives of a company, such as bus drivers and plane pilots, who are authorized to use CBP One™ to submit manifest information to CBP. Sea, land, and air operators will be able to use CBP One™ to submit information to CBP on behalf of consenting travelers through applications, such as the I-94 mobile application. Operators will use the application to gather information from travelers in order to bulk submit information to CBP. Operator capabilities will not be available in CBP One™ at launch. Once operator functionality launches, CBP will create an appendix to this PIA and, as necessary, publish a standalone PIA Update documenting the new features.

International Organizations

CBP has formed partnerships with International Organizations to assist aliens seeking admission into the United States. Access to the International Organization functionality within

CBP One™ is limited to International Organizations identified by the United States Department of State (DoS) as having established roles supporting the Government of Mexico to provide services to MPP enrollees. If the user is not a verified International Organization, the individual will not see the International Organization persona in the list of options on the CBP One™ homepage. Appendix C of this PIA provides additional guidance on the use and functionality of the International Organization feature and CBP is developing a standalone, function-specific PIA for the MPP program.

Information Collected

The information users provide to CBP depends on the function of CBP One™ that they are using. For example, individuals using CBP One™ to report their travel into and out of the United States have to provide more information than users scheduling agriculture inspection appointments. Users will have to provide basic biographic information, such as first and last name, contact information, and email address, in order to create a Login.gov account and use the application. Regardless of the function, CBP One™ does not store any information locally on the device. CBP pushes all information collected through CBP One™ to back-end systems associated with the functions the user is using. For example, CBP will store information related to I-94 information submitted through CBP One™ in CBP's I-94 databases.

Compliance Framework

In its initial phase, CBP One™ is operational for users to schedule an agricultural inspection or apply for an I-94 prior to arrival. CBP One™ will continue to expand to become the unified mobile portal for public transactions with CBP. CBP is conducting this overarching PIA to describe the risks and mitigations associated with CBP One™; however, due to broad and disparate functions contemplated for CBP One™, CBP will conduct standalone, function-specific PIAs for each function as necessary. CBP will add or update the Appendices to this PIA as new functions are developed to ensure transparency regarding all publicly available CBP mobile applications.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[5] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure

[5] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[6]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[7] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[8] and the Homeland Security Act of 2002, Section 222.[9] Given that CBP One™ is a portal rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of CBP One™ as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

CBP One™ is a publicly available mobile application available for Android and iOS mobile devices in the Google Play or iTunes mobile application stores. To promote transparency and provide notice to the public of this new mobile portal to CBP services, CBP published a press release when CBP One™ was launched to the public.[10] The release detailed the functions available at launch as well as the functions that CBP plans to roll out in the future. CBP is also working with industry to provide additional information about CBP One™. CBP will continue to provide information to the public through the use of flyers and outreach to industry groups. CBP may conduct targeted outreach for specific functions, and may conduct standalone, function-specific PIAs for new functions as necessary for additional transparency.

There is no privacy risk to transparency; CBP One™ is public-facing and voluntarily available for the public to use.

---

[6] 6 U.S.C. § 142(a)(2).
[7] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[8] 44 U.S.C. § 3501 note.
[9] 6 U.S.C. § 142.
[10] *See* U.S. CUSTOMS AND BORDER PROTECTION, CBP ONE™ MOBILE APPLICATION (June 28, 2024), *available at* https://www.cbp.gov/about/mobile-apps-directory/cbpone.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Anyone may voluntarily download CBP One™ from the mobile application store on his or her mobile device. While CBP One™ is limited in its initial functionality, it is available for any traveler or entity that needs to interact with CBP, so long as the mobile application supports the function that the user is trying to complete.

In addition, CBP One™ contains a privacy policy that appears every time a user logs in. Users must consent to the terms of using the application prior to being authorized to use it. CBP reserves the right to make changes to the privacy policy by giving notice to its travelers on the CBP One™ Mobile App privacy policy page, and by ensuring protection of PII in all cases. CBP strongly recommends visiting the CBP One™ Mobile App privacy policy page, and referring to the dates of the modification. Additionally, CBP will place a banner notice on the app landing page to notify users that CBP has updated the privacy policy. Depending on the functionality, if applicable, CBP One™ also uses "just-in-time" notifications that require users consent before the application can access camera or GPS functions, for example.

Some functions of CBP One™ allow users to submit information on behalf of other people. This may include a family member submitting information on behalf of another, to the extent authorized by law. For example, a parent could submit an exit or request travel history on behalf of his or her minor child. In other functions an operator or International Organization collect information from individuals and submit that information to CBP, through CBP One™. For example, a bus operator may collect information from travelers and submit that information to CBP through CBP One™ in order to report the traveler's entry or an International Organization may collect information on behalf of aliens seeking admission to the United States, typically as part of a formalized program such as MPP. International Organizations and Operators are responsible for notifying individuals about information collected and submitted to CBP through CBP One™.

Because CBP One™ does not store any information, there are no records to correct or amend. If users submit 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. Additionally, travelers may request information about records contained in the source systems that CBP One™ populates through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)) online at https://foia.cbp.gov/palMain.aspx or by writing to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

When seeking records, the request must conform to Part 5, Title 6 of the Code of Federal Regulations. An individual must provide his or her full name, current address, and date and place of birth. The individual must also provide:

- An explanation of why the individual believes DHS would have information on him or her;
- Details outlining when the individual believes the records would have been created; and
- If the request is seeking records pertaining to another living individual, a statement from that individual certifying his or her agreement for access to his or her records.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this information, CBP may not be able to conduct an effective search and the request may be denied due to lack of specificity or lack of compliance with applicable regulations. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

Privacy Risk: There is a risk that a user could submit information about another individual(s), without receiving prior consent from the individual(s).

Mitigation: This risk is partially mitigated. Although CBP cannot prevent users from submitting information for other users, there is no discernable benefit for a user to do so. Additionally, the user would have to have access to another person's biographic information and in some cases, travel documents. Some functions of CBP One™, like the I-94 mobile application, also require users to submit photographs of themselves and co-travelers. CBP is able to verify if the photograph is of a "live" person; if it is not, the transaction cannot proceed.

In addition, specific privacy risks related to individual participation will be addressed in standalone, function-specific PIAs.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

CBP One™ allows users to interact with CBP for a variety of purposes. Regardless of function, users will have to provide basic biographic and contact information in order to use the application. Brokers/carriers/forwarders have to submit business information, such as company name and importer ID, in addition to the user's own biographic information, such as name and email address, in order to schedule inspections. CBP One™ users reporting exit and entry information will provide additional biographic information that CBP will use to verify identity and identify derogatory information. With user consent, CBP One™ may also capture geolocation information from users' devices. Different functions may also require users to submit "live" photographs of themselves. The standalone, function-specific PIAs will fully discuss the information CBP uses to perform the required function.

CBP One™ allows users to perform a variety of functions. Because the profile creation is done through Login.Gov, CBP One™, as an umbrella application, does not store information on users. Consistent with the Import Information System SORN,[11] brokers/carriers/forwarders can submit information to and interact with CBP to schedule cargo inspections. CBP's Border Crossing Information (BCI)[12] and Arrival and Departure Information System (ADIS)[13] SORNs govern the information CBP One™ users provide when attempting to enter and exit the United States. CBP's Automated Targeting System (ATS),[14] Border Patrol Enforcement Records (BPER),[15] and the U.S. Customs and Border Protection TECS[16] SORNs govern the information undocumented individuals provide through CBP One™ in advance of their arrival at a port of entry.

Specific privacy risks related to purpose specification will be addressed in standalone, function-specific PIAs.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

---

[11] *See* DHS/CBP-001 Import Information System, 81 Fed. Red. 48826 (July 26, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[12] *See* DHS/CBP-007 Border Crossing Information (BCI), 81 Fed. Reg. 89957 (December 13, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[13] *See* DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 Fed. Reg. 72081 (November 18, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] *See* DHS/CBP-006 Automated Targeting System (ATS), 80 Fed. Reg. 13407 (March 13, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.
[15] *See* DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[16] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

The retention of information CBP collects through CBP One™ depends on the function the individual is using. CBP uses information collected through CBP One™ to populate existing CBP systems. For example, information provided by brokers/carriers/forwarders to schedule inspections is stored in a database within the Automated Commercial Environment for 1 year in accordance with the Import Information System SORN. Whereas information used to report a traveler's exit from the United States may be stored in ADIS for 75 years.

Specific privacy risks related to data minimization will be addressed in standalone, function-specific PIAs, including the relevant data retention period for the information. No information is stored locally on the user's device or in the CBP One™ application itself.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

CBP uses Login.gov to provide a secure and credentialed way for CBP One™ users to access the application and its different functions. CBP One™ allows users a single easy to use portal through which to conduct a variety of transactions with CBP. CBP uses information provided by brokers/carriers/forwarders to schedule inspection appointments and request additional information. CBP uses other traveler-provided information in order to vet travelers, update systems, and display relevant information to travelers. CBP uses geolocation information to determine whether functions, such as reporting exit and arrival, can be accessed by the user, and to confirm whether or not the individual is in the 1-mile pertinent radius reporting requirement.[17] CBP uses photographs submitted by users in order to validate identity and that the person is "live", employing liveness detection capabilities. CBP will publish standalone, function-specific PIAs for certain functions within CBP One™.

CBP may share information collected through CBP One™ both inside and outside of DHS consistent with applicable law and policy. However, no sharing will come directly from CBP One™. Any sharing is done from the system in which the information resides, pursuant to the applicable SORNs that govern that system and associated information sharing arrangements. Primarily, CBP would share information collected through CBP One™ for vetting purposes. Standalone, function-specific PIAs will fully discuss function-specific sharing.

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 travelers or to track traveler's movement.

[17] For inbound vessels, CBP does not allow travelers to report their arrival until they are within 1 mile of the U.S. border. Similarly, CBP requires travelers to be at least 1 mile outside of the U.S. border to report their exit.

Mitigation: This risk is fully mitigated. The geolocation information collected from CBP One™ users will not be used to conduct surveillance or track traveler's movement. CBP does not track the location of the traveler's device beyond the time of submission of the data. At the time the user submits his or her exit or entry, the device's GPS is pinged by CBP One™ and the latitude and longitude coordinates are sent to CBP. The GPS ping is only collected at the exact time the user pushes the submit button and is used to confirm the traveler's device is in some cases inside a certain CBP-defined radius or outside the United States. The latitude and longitude information captured is not visible to CBP Officers or Agents. CBP collects the latitude and longitude information from the GPS ping and uses this information for analytical purposes (e.g., to determine that the individual is in the 1-mile radius pertinent reporting requirement for the report of arrival of pleasure boats through CBP ROAM or outside of the United States for exit).

In addition, any specific privacy risks related to use limitation will be addressed in any standalone, function-specific PIAs.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

CBP One™ collects information directly from users who are voluntarily using the application. A user must consent to a Privacy Policy each time CBP One™ launches. Users can manually enter information or use their device's camera to scan the Machine-Readable Zone of a travel document, which will prepopulate information into CBP One™. Depending on the function, CBP may check information submitted by the user against CBP holdings to verify that the information matches already existing information. Users have an incentive to provide CBP with accurate information because users have chosen to voluntarily interact with CBP through CBP One™ and are seeking some form of service from CBP. Some users may submit information on behalf of others; for example, a family member submitting information for another family member, to the extent authorized by applicable law and policy. Additionally, operators may use CBP One™ to submit arrival and departure information for their passengers and crew to the extent authorized. Operators who submit information about travelers to CBP through CBP One™ are responsible for notifying travelers about their collection and sharing of the information with CBP. Operators generally provide this notice during their ticketing process. International Organizations provide notice to individuals before submitting information to CBP on their behalf.

In some cases, CBP One™ obtains consent from users to view GPS location at time of submission. This ensures that entries and exits are accurately submitted and prevents users from attempting to claim they have departed the United States when they are still in the United States. Additionally, for some functions CBP requires users to submit a photograph of the person whose information is being captured by CBP One™. CBP uses photographs submitted by its users to

validate identity, match against CBP holdings, and determine whether the photograph is "live". The liveness detection capabilities provide validation that an individual is present at the time of submission.

Privacy Risk: There is risk that users will submit inaccurate information about other people.

Mitigation: This risk is fully mitigated. Although CBP cannot prevent users from submitting inaccurate information on behalf of themselves or other people, CBP can verify the information before retaining it as accurate. It is unlikely that a user will submit inaccurate information on about another person. Primarily, because there is no benefit in submitting inaccurate information through CBP One™. In some cases, the submission of the inaccurate information could subject the user to monetary or legal penalties. CBP verifies that the biographic information is correct and depending on the function can verify the identity of a person and their location.

In addition, any specific privacy risks related to data quality and integrity will be addressed in any standalone, function-specific PIAs.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

The CBP One™ mobile application uses Login.gov to manage users' authentication by allowing users to sign in with an email address, password, and multi-factor method, and conduct identity proofing by verifying an individual's asserted identity. Login.gov ensures a secure connection and identity verification when using the CBP One™ mobile application. Individuals with a Login.gov account can sign into multiple government websites (including CBP One™) with the same email address and password. Login.gov does not share any information provided by the user with CBP.

No information is stored locally on the user's device or in the CBP One™ application itself. The retention of information CBP collects through CBP One™ depends on the function the user is using. CBP uses information collected through CBP One™ to populate existing CBP systems. In turn, the security controls of those systems protect the information. For example, information provided by brokers/carriers/forwarders to schedule inspections is stored in a database within the CBP Amazon Web Services (AWS) Cloud East (CACE) and is protected by the CACE security controls. Additionally, 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 functions.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

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. CBP One™ only stores the users Login.gov email address locally onto the user's device. All other information submitted by the user through CBP One™ is sent to existing CBP source systems. The CBP source systems where information is stored maintain their own auditing and accountability capabilities that will be more fully explained in the appendices as functions launch, as well as in any standalone, function-specific PIAs. Further, all CBP employees are required to complete the DHS Security Awareness Training Course and privacy training which explains how to properly handle and protect PII.

Conclusion

The CBP One™ mobile application is a secure, mobile portal for the public to conduct various transactions with CBP. In its initial phase, CBP One™ is operational for users to schedule an agricultural inspection or report their departure from the United States, in accordance with law. CBP One™ will continue to expand to become the unified mobile portal for public transactions with CBP. CBP conducted this overarching PIA to describe the risks and mitigations associated with CBP One™; however, due to broad and disparate functions contemplated for CBP One™, CBP will also conduct standalone, function-specific PIAs for certain privacy-sensitive functions. CBP will add links and summaries of each new functional PIA to the Appendices as they are published to ensure transparency on all publicly available CBP mobile applications.

Responsible Official

Jody Hardin
Director, Strategic Transformation Office, Office of Field Operations
U.S. Customs and Border Protection
U.S. Department of Homeland Security

Debra L. Danisek
CBP Privacy Officer, Privacy and Diversity Office
U.S. Customs and Border Protection
U.S. Department of Homeland Security
Privacy_CBP@cbp.dhs.gov

Approval Signature

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

_____

James Holzer
Acting Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

APPENDIX A: Travelers

Updated July 25, 2024

1. I-94 Mobile

I-94 Mobile is function of CBP One™ and offers the same features as the current CBP I-94 website (i.e., allows nonimmigrant aliens to apply for a provisional I-94, pay in advance of arrival for an I-94, retrieve their most recent I-94, view their travel history, and check their authorized period of stay on any active I-94). I-94 Mobile provides the convenience to capture travel document information via an optical character recognition scan to auto-populate the information into the travel document fields when adding one's travel document information.

Additionally, I-94 Mobile will provide a traveler the ability to self-report the traveler's exit from the United States. CBP plans to pilot the self-reporting exit feature in Spring 2021, at select locations along the Northern Border. The population that can volunteer to use the I-94 Mobile features for self-reporting departures is limited to I-94 travelers who have come temporarily to the United States and are exiting the United States at the Pacific Highway and Peace Arch Border Crossing located in Blaine, Washington; the Champlain-St. Bernard de Lacolle Border Crossing located in Champlain, New York; and the Ambassador Bridge and Detroit-Windsor Tunnel located in Detroit, Michigan. CBP is conducting the pilot at these locations on the Northern Border due to CBP's partnership with the Canadian Border Services Agency (CBSA). If successful, CBP hopes to expand the Self-Reporting Mobile Exit (SRME) function of I-94 Mobile to the Southern Border to increase the accuracy of CBP exit records. CBP will publish a standalone, function-specific Privacy Impact Assessment that discusses the Voluntary Self-Reporting Mobile Exit function in more detail and also update the existing I-94 Privacy Impact Assessment series to include the CBP One™ mobile application as a way in which individuals can apply for and check their I-94s.

2. Reporting Offsite Arrival-Mobile (ROAM)™

The Reporting Offsite Arrival – Mobile (ROAM)™ functionality is embedded into the CBP One™ mobile application and provides travelers arriving to the United States with an option to voluntarily self-report their arrival to CBP. In addition, the Reporting Offsite Arrival-Mobile mobile functionality will automate existing manual data entry and law enforcement queries for CBP and provide a more sophisticated capability for conducting a remote inspection via video conference. This function will not be available at launch of CBP One™; CBP will publish a standalone, function-specific Privacy Impact Assessment to discuss the privacy risks and mitigations thoroughly. CBP will update this Appendix when the standalone Privacy Impact Assessment is published.

3. Collection of Advance Information from Certain Undocumented Individuals Traveling to the Land Border

CBP One™ allows certain undocumented individuals[18] who lack documents sufficient for admission to the United States to submit information to CBP in advance of their arrival at a land port of entry. This functionality, available under the "Submit Advance Information" tab within the "Land" section in the "Traveler" persona, allows certain undocumented individuals to voluntarily submit biographic information, as well as a facial photograph, to CBP in advance of their arrival at the port of entry. Typically, once an undocumented individual arrives at a land POE for processing, CBP officers spend significant time collecting and verifying basic biographic data about the individual during the inspection process. One at a time, the CBP officers interview and collect information from such individuals during secondary inspection. The CBP officers manually enter the information into the Unified Secondary System (USEC).[19]

To streamline and increase processing capacity at land ports of entry, CBP uses the CBP One™ mobile and desktop applications to allow the advance submission of biographic and biometric information from undocumented individuals seeking admission into the United States. CBP One™ data is displayed to CBP officers through the primary inspection screen and is made available for importation into the Unified Secondary System as an immigration event. Once the individual is logged in to CBP One™, they are prompted to select "Traveler," then "Land," then "Submit Advance Information." First time users will be prompted to select their preferred language).[20] After these steps are complete, the user must then select "Add Individual." CBP One™ then collects the same information that CBP would otherwise collect during the primary and/or secondary inspection, including:

- Facial photograph;
- First and last name;
- Date of birth;
- Nationality;

[18] An undocumented individual is a noncitizen who does not possess a document valid for admission to the United States. 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).

[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR U.S. CUSTOMS AND BORDER PROTECTION UNIFIED SECONDARY, DHS/CBP/PIA-067 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[20] Currently CBP One™ is available to users in both English, Spanish, and Haitian Creole. In future releases of CBP One™, the languages will be expanded to include additional languages.

- Country/city of birth;
- Country of residence;
- Travel document information;
- Phone numbers;
- U.S. address;
- Foreign addresses (optional);
- Employment history (optional);
- Travel history (optional);
- Emergency contact information (optional);
- Family information;
- Marital information;
- Identity documents ((optional);
- Gender;
- Height;
- Weight;
- Eye color;
- Requested Date/Time of Arrival (required to schedule); and
- Intended arrival port of entry(required to schedule).

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

CBP One ™ will also collect latitude and longitude coordinates. These coordinates will be sent to CBP to determine whether the submission is occurring within a CBP-defined proximity to the U.S.-Mexico border. In addition, CBP One™ collects the preparer's (person assisting the individual with their submission) first and last name and email address.

a. Uniting for Ukraine

On April 25, 2022, the direct land traveler advance information capability was made available to eligible Ukrainian citizens and, as appropriate, members of their immediate family, who have an approved advance authorization to travel to the United States to seek parole pursuant

to the Uniting for Ukraine (U4U) process.[21] Such individuals are able to use the application to schedule a date and time to present themselves for inspection at a land port of entry. Additional information related to CBP's screening and vetting process as part of Uniting for Ukraine was provided in the Automated Targeting System (ATS) Privacy Impact Assessment Update Addendum 2.8.[22] DHS, in partnership with the Department of State, provides local messaging in Mexico to individuals who may need to utilize CBP One™ to schedule a date and time to arrive at a port of entry following a Uniting for Ukraine travel authorization approval. The messaging encourages individuals with an approved advance travel authorization to arrive to the United States via commercial flight, but also encourages those who intend to travel to a U.S.-Mexico land border port of entry to use CBP One™ to request a date and time to present.

b. Processing of Undocumented Individuals while Title 42 is in effect (ended May 11, 2023)

This process for Undocumented Individuals is no longer in effect due to the termination of the Title 42 Order. However, CBP is keeping reference to the functionality within this Privacy Impact Assessment for historical purposes. Information about that effort is below.

On January 12, 2023, CBP expanded the advance information submission functionality to certain undocumented individuals who seek to travel to the United States through southwest border (SWB) land POEs to request an exception to the Centers for Disease Control and Prevention (CDC) Order, "*Suspending the Right to Introduce Certain Persons from Countries Where a Quarantinable Communicable Disease Exists* (hereafter referred to as Title 42)."[23]

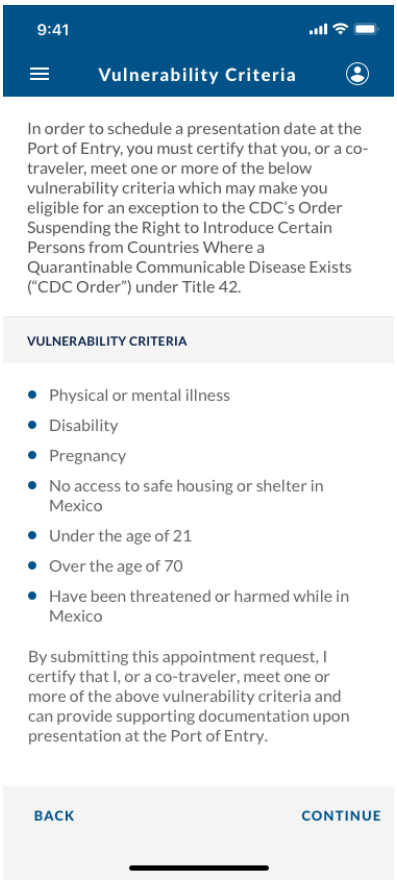
---

[21] *See* Press Release titled "President Biden to Announce Uniting for Ukraine, a New Streamlined Process to Welcome Ukrainians Fleeing Russia's Invasion of Ukraine," *available at* https://www.dhs.gov/news/2022/04/21/president-biden-announce-uniting-ukraine-new-streamlined-process-welcome-ukrainians.

[22] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006(e) (2022), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection. CBP is currently developing an update to this Privacy Impact Assessment to discuss the collection of geolocation data to ensure an individual is within a certain range of the U.S.-Mexico border.

[23] 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 Centers for Disease Control and Prevention 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.

While the Title 42 Order is in effect, undocumented individuals seeking to travel to the United States through a Southwest Border port of entry 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.



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

- Physical or mental illness;
- 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 eligible to submit advance information to CBP, the user must attest that they believe that they and their spouse and/or children meet the vulnerability criteria. If the user attests that they believe that they meet the above vulnerability criteria, the user may enter the biographic and biometric information into CBP One™ and schedule an appointment to present themselves at a participating port of entry to request an exception from the Title 42 Order.[24,25] All undocumented individuals seeking an exception

[24] At the time of publication, the participating ports of entry are Nogales, Brownsville, Eagle Pass, Hidalgo, Laredo, El Paso (Paso del Norte), Calexico, and San Ysidro.
[25] *See* 86 Fed. Reg. 53667 (September 28, 2021). 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. 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 ports of entry. 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.

to Title 42 and submitting information through CBP One™ are required to be within a CBP-defined proximity to the U.S.-Mexico border (as determined by the phone's GPS at the time of submission) and must complete liveness detection through their device's camera[26] in order to schedule a date and time to present, to assist in streamlining the processing upon arrival at a port of entry. Use of CBP One™ does not guarantee that an individual will be granted an exception to the Title 42 Order.

For all individuals accessing CBP One™ on a mobile device and who are located within the CBP-defined proximity to the U.S.-Mexico border, once the individual has entered all biographic information as well as a facial photograph for themselves, spouse and/or children, the user is required to select a desired port of entry and desired date of arrival, and desired time of arrival. All individuals accessing CBP One™ on the web will be required to submit the facial photograph as well as the other biographic information through the web; however, they will be instructed to utilize the mobile application to select available arrival date/times. All individuals utilizing CBP One™ to schedule or reschedule a presentation date after their initial submission will be required to submit a live facial photograph to access their original submission. CBP uses 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[27] capabilities within the photograph to ensure mobile device is being used by a "live person" who is requesting to schedule their arrival at a port of entry.

While CBP allows individuals to select a desired port of entry and date/time of arrival, this request does not 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 port of entry's capability to do so. The scheduling feature helps CBP to properly allocate resources to the port of entry's for a given day or week to further assist in streamlining in-person processing upon arrival. Once a port of entry 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 port of entry and date/time, if applicable. A copy of the confirmation is also sent to the email address(es) provided under contact information during the CBP One™ submission, or, in the absence of an email within CBP One™, to the registered email of the Login.gov account.

Prior to arrival at the port of entry, CBP may use the information submitted by the individual to conduct system checks to identify individuals who may pose a risk to national

[26] CBP did not conduct liveness detection during the initial launch phase that involved only those with approved advance authorizations to travel to the United States to seek parole under Uniting for Ukraine.
[27] 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.

security, border security or public safety. These checks are identical to the checks conducted by CBP during the primary or, in some cases, secondary inspection process.[28] CBP will not inform the user of the outcome of these checks, but CBP officers will use the information during primary and secondary inspections.

During primary inspection at the port of entry, the CBP officer will use the Simplified Arrival system to take a new facial photograph.[29] This facial photograph is searched against the CBP Traveler Verification Service's (TVS) pre-staged "Submit Advance Information" gallery, which consists of templates from the facial photograph submitted by users during the submission process. If there is a match, the information the user submitted through CBP One™, as well as the results of the system checks, will be displayed to the officer. If no match is made, officers will manually enter the individual's confirmation number or biographic data to populate Simplified Arrival for processing in primary. As with any individual who arrives at the port of entry without documentation, the officer will use Simplified Arrival to create a referral to secondary for further processing, to include the confirmation number received from CBP One™. Once referred to secondary, CBP Officers may import the information captured through the CBP One™ application into a Unified Secondary event.

c. Processing of Undocumented Individuals post-Title 42 (effective May 11, 2023, 11:59PM Eastern Standard Time)

On January 30, 2023, in response to a pending bill that would immediately terminate both the public health emergency and a separate COVID-19 national emergency declared by the President, the Office of Management and Budget issued a statement opposing such an immediate termination but announcing that "[a]t present, the Administration's plan is to extend the emergency declarations to May 11, and then end both emergencies on that date."[30] The currently operative Title 42 order states that it automatically ends upon the expiration of that declaration.[31] Therefore, if the public health emergency declaration expires on May 11, 2023, the Title 42 order will have expired by its own terms.

---

[28] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates), and U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[29] *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.

[30] *See* Office of Management and Budget, *Statement of Administration Policy* 1 (Jan. 30, 2023), *available at* https://www.whitehouse.gov/wp-content/uploads/2023/01/SAP-H.R.-382-H.J.-Res.-7.pdf.

[31] 86 Fed. Reg. 42828, 42830 (Aug. 5, 2021).

Following the termination of the Title 42 order, CBP is returning to processing all individuals under Title 8 of the U.S. Code. Undocumented noncitizens will be able to use CBP One™ to schedule a date and time to be processed at a port of entry. However, such noncitizens will not be required to attest to any vulnerability criteria to schedule an appointment, as CBP will process all noncitizens arriving at ports of entry, regardless of vulnerability.[32]

In addition to the removal of the vulnerability criteria that occurred on April 29, 2023, CBP is making significant enhancements to the scheduling functionality within CBP One™, which will be effective as of May 10, 2023. CBP One™ users and stakeholders continue to report frustration and stress, particularly related to a process that requires all users to access the application at the same time and attempt to schedule a limited number of available appointments. Most importantly, CBP is concerned about the reports of potential fraud and exploitation related to the current process.

With this update, users will no longer be required to access the application at the same time each day to select a port of entry and schedule an appointment. Instead, users will now be able to, once each day at the time that is best for them, request an appointment (for up to 13 days later). Once the user requests an appointment, they will be put into a pool of registrations, and appointments will be allocated on a daily basis. Thus, the user will be notified the following day if they were allocated an appointment. CBP will use an algorithm to allocate daily appointments to undocumented individuals who request an appointment each day. In the event an individual is not allocated an appointment, they must request an appointment again to be considered for the next day's allocation. Individuals who are offered an appointment are notified that they were allocated an appointment through an email notification, a push notification to the device that requested the appointment, an in-app message that will display when they access the application, and an update to their registration status within the CBP One™ application. After this notification is sent, the individual is given 23 hours to confirm the appointment by completing the photo capture and liveness detection process as described in the Collection of Advance Information from Certain Undocumented Individuals on the Land Border Privacy Impact Assessment.[33] Any appointment that is not confirmed within the allotted timeframe will be reallocated with the daily allocation for

[32] Additionally, DHS and DOJ are considering publication of a Final Rule that will, apply a rebuttable presumption of asylum ineligibility to noncitizens who, during a temporary period of time, do not use a safe, orderly and lawful pathway to the United States, including use of the CBP One™ app to schedule an appointment to present at a port of entry, unless the noncitizen demonstrates by a preponderance of the evidence that it was not possible to access or use CBP One™ due to a language barrier, illiteracy, significant technical failure, or other ongoing and serious obstacle; or that the noncitizen is otherwise not subject to exception from or can rebut the rebuttable presumption. *See* https://www.federalregister.gov/documents/2023/02/23/2023-03718/circumvention-of-lawful-pathways.

[33] If an individual is experiencing technical difficulties, they are able to request an automatic extension through the application of another 23 hours. If they still have not resolved their issue, they will need to ask for an appointment again.

that current day until all appointments are filled up until 3 days from arrival.[34]

CBP concurrently published a standalone Privacy Impact Assessment titled "Collection of Advance Information from Certain Undocumented Individuals on the Land Border"[35] and subsequent updates to provide full transparency on this initiative and fully assess the risks associated with CBP's collection of information from undocumented individuals in advance of their arrival at port of entry.

d. Advance Authorization to Travel to the United States to Seek a Discretionary Grant of Parole or Family Reunification Parole for Certain Undocumented Noncitizens from Select Countries

DHS has created a new Advance Travel Authorization (ATA) process[36] to provide certain undocumented noncitizens from select countries the opportunity to request advance authorization to travel to the United States to seek a discretionary grant of parole. The Advance Travel Authorization process provides a streamlined way for certain noncitizens to submit personal information to USCIS and CBP to facilitate the issuance of an advance authorization to travel to the United States to seek a discretionary grant of parole.

Persons or entities legally physically present in the United States may submit a Form I-134, *Declaration of Financial Support*, or Form I-134A, *Online Request to be a Supporter and Declaration of Financial Support*, to USCIS on behalf of an individual beneficiary potentially eligible to receive advance travel authorization under this process. Following approval of the Form I-134 or I-134A, 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.[37] Travelers use their myUSCIS account to verify their biographic information as provided on Form I-134 or I-134A is accurate and to attest to all requirements. Once the traveler has confirmed their biographic information, myUSCIS will inform the traveler to complete their request for advance authorization

[34] This cutoff is to reduce late notifications for families and individuals to prepare for presentation at the port of entry.
[35] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE COLLECTION OF ADVANCE INFORMATION FROM CERTAIN UNDOCUMENTED INDIVIDUALS ON THE LAND BORDER, DHS/CBP/PIA-076 (2023 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[36] *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 (2022 and subsequent updates), *available at* https://www.dhs.gov/privacy-impact-assessments.
[37] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICE, PRIVACY IMPACT ASSESSMENT FOR THE MYUSCIS ACCOUNT EXPERIENCE, DHS/USCIS/PIA-071 (2018 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

to travel by downloading and using the CBP One™ mobile application to submit biographic and biometric data.

The traveler must log into CBP One™ and 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 direct the user to "Scan Passport." The CBP One™ mobile application will 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, software determines whether there is a readable eChip[38] embedded 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 date of birth, passport number, and nationality. This information is then automatically populated into the submission of the mobile application to eliminate the need for manual input by the traveler.

Following the collection of this information, users who have eChips will then 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[39] 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.

CBP One™ collects and sends the A-Number, date of birth, and passport number to the CBP Arrival and Departure Information System (ADIS) in order to verify that the traveler accessing the specific functionality within CBP One™ has a USCIS-approved, U.S.-based supporter and has verified their biographic information and has provided the DHS-required attestations related to program eligibility criteria.[40] The Arrival and Departure Information System

[38] 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 (VWP) 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.
[39] 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.
[40] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT

directly interfaces with the USCIS Electronic Immigration System (ELIS), used to process immigration benefits.[41] 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 date of birth, nationality, sex, A-Number, passport number, and passport expiration date to the Automated Traveler Information System (ATIS) for vetting.[42] 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.[43] If CBP cannot confirm that the traveler has been approved by USCIS for Advance Travel Authorization or identify a valid passport, the traveler will not be able to complete their request for advance authorization to travel.

Once the biographic and eChip data is collected, CBP One™ prompts the user to take a live photograph or selfie (new photograph and not the same image collected from the passport/e-passport). CBP One™ instructs the user to line their face up with a circle on the screen of their mobile device. CBP One's™ embedded software then performs a "liveness" test to determine that it is real person (and not a picture of a person).[44] CBP One™ allows the user to capture their image and select "Continue" once they are satisfied it is an accurate photo. CBP One™ will reject any images that are not correctly captured, such that only one live photograph is collected. 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 entered incorrectly. Once the user verifies and submits their information, the data and photographs are passed to the downstream

---

ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS) , DHS/CBP/PIA-024, *available at* https://www.dhs.gov/privacy-impact-assessments.

[41] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC IMMIGRATION SYSTEM (USCIS ELIS), DHS/USCIS/PIA-056, *available at* https://www.dhs.gov/privacy-impact-assessments; and DHS/USCIS-007 Benefits Information System, 81 FR 72069 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

[42] The Automated Traveler Information System (ATIS) 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.

[43] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates), and U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[44] While the user is taking the "selfie," the technology embedded within the mobile application relies on the devices 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.

systems described below. The CBP One™ application will advise the user to refer to their myUSCIS account for further information regarding their request.

Once all the required information and a new live photograph are submitted, the information is saved in the Automated Traveler Information System and copied to CBP's Automated Targeting System/Unified Passenger system (ATS-UPAX) 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).[45,46] 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.

Uses of Facial Comparison in Downstream System During Advance Travel Authorization Process:

CBP uses facial comparison technology at various stages in the Advance Travel Authorization process.

Although CBP One™ does not conduct any facial recognition activities, 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 Advance Travel Authorization mobile application 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 Advance Travel Authorization vetting process; (3) to generate a new gallery of Advance Travel Authorization participants for facial comparison when Advance Travel Authorization 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.

---

[45] *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 and subsequent updates), *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.

[46] However, a traveler's 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. More information about this advance traveler authorization and the process at ports of entry *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Retention of Data

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.[47] The selfie photograph collected through CBP One™ is passed to downstream systems and is not stored in the CBP-owned cloud. CBP will store this photograph in the Automated Targeting System and the Advance 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), but not more than 180 days. 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. In addition, CBP One™ collects the first and last name of the user as part of the profile creation. 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. CBP is concurrently developing a standalone Privacy Impact Assessment to fully explain the Advance Traveler Authorization process.[48]

[47] The aggregate data used for reporting are covered by the following records schedule: General Records Schedule (GRS) 5.2, item 020. Intermediary Records. Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. The reports submitted to CBP Leadership that are generated from the aggregate data are covered by the following records schedule: DAA-0563-2019-0008-0003. Periodic Reports. Temporary. Cutoff at the end of the calendar year. Destroy five years after cut-off.

[48] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR ADVANCE TRAVELER AUTHORIZATION, DHS/CBP/PIA-073 (2022), *available at* https://www.dhs.gov/privacy-impact-assessments.

APPENDIX B: Stakeholder Requests for CBP Services

Updated July 25, 2024

1. Stakeholder Scheduling

The Stakeholder Scheduling functionality is embedded into the CBP One™ mobile application, and provides a mobile and web option for brokers, carriers, forwarders, and travelers to quickly request an inspection of personal goods, commercial vessels, or cargo entering the United States with agricultural and biological products, view real time appointment status updates, view inspection request history, and interact with a CBP Agricultural Specialist via a chat feature embedded into the mobile and desktop application.

The scheduling functionality reduces wait time, enhances communication between CBP and the broker/carrier/forwarder, and streamlines the inspection process at ports of entry.

2. Scheduling Dashboard

CBP employees, CBP Officers, and Agriculture Specialists use the CBP Scheduling dashboard to manage incoming inspection requests from travelers with permitted goods and brokers with permitted cargo. The CBP Scheduling dashboard is accessible via a computer workstation, laptop, or tablet and will directly connect to CBP One™. The internal CBP Scheduling dashboard is not accessible to members of the public. Data submitted by the public through the CBP One™ application's Scheduling functionality is transferred to the internal Scheduling dashboard. CBP Officers and CBP Agricultural Specialists permitted access to the internal CBP Scheduling dashboard can view data that was submitted through the CBP One™ application's Stakeholder Scheduling functionality by travelers and brokers and manage those requests. The Scheduling dashboard displays information submitted by users via CBP One™, such as personal effects, cargo and/or commercial vessel details, and the date the inspection should be performed.

The Scheduling dashboard can also be used internally between CBP employees and CBP supervisory employees concerning the Stakeholder Scheduling process. This includes using the dashboard to assign CBP employees to an inspection and changing inspection statuses to indicate progress (e.g., "Pending", "Acknowledged", "Doc Reviewed", "Scheduled", "Assigned", "Enroute", "Completed," "Canceled"). CBP employees may edit inspection and cargo/vessel details displayed as needed, and make notes or comments for a request in the "Internal Notes" section.

APPENDIX C: Non-Governmental Organizations

Updated July 25, 2024

1. Migrant Protection Protocol

2024 updates

DHS first sought to terminate the Migrant Protection Protocols (MPP) program in a June 2021 memorandum. In August 2021 the U.S. District Court for the Northern District of Texas enjoined the program termination in *Texas v. Biden*, No. 2:21-cv-067, 2021 WL 3603341 (N.D. Tex. Aug. 13, 2021). DHS terminated the program in a subsequent October 2021 memorandum that superseded the June 2021 memorandum and directed that termination be implemented as soon as practicable after a final judicial decision to vacate the *Texas* injunction. The District Court vacated the *Texas* injunction in August 2022, following a related U.S. Supreme Court ruling, and in December 2022, the District Court issued a decision staying the Secretary's October 2021 memoranda terminating Migrant Protection Protocols pending final resolution of the merits of the case. CBP turned off access to the Non-Governmental Organization (NGO) Case Check functionality on January 25, 2023, but is keeping reference to the functionality within this Privacy Impact Assessment for historical purposes.

May 2021

In early 2019, CBP began implementing the Migrant Protection Protocols,[49] which is a U.S. government action whereby certain foreign individuals from countries other than Mexico, without proper documentation, entering or seeking admission to the United States by land from Mexico are returned to Mexico to wait outside of the United States for the duration of their immigration proceedings. In January 2021,[50] the United States suspended new enrollments into Migrant Protection Protocols and, in February 2021, began the process of permitting foreign individuals previously in Migrant Protection Protocols to be processed into the United States. In order to enroll individuals in Migrant Protection Protocols, CBP used Unified Secondary[51] and

[49] *See* Policy Guidance for Implementation of the Migrant Protection Protocols (January 25, 2019), *available at* https://www.dhs.gov/sites/default/files/publications/19_0129_OPA_migrant-protection-protocols-policy-guidance.pdf.

[50] *See* Executive Order 14010, Creating a Comprehensive Regional Framework To Address the Causes of Migration, To Manage Migration Throughout North and Central America, and To Provide Safe and Orderly Processing of Asylum Seekers at the United States Border (February 3, 2021), *available at* https://www.federalregister.gov/presidential-documents/executive-orders.

[51] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT

e3[52] to collect a photograph and biographic information from the individual. CBP stores this information in a CBP database in the Enforcement Integrated Database (EID).[53]

CBP is working with International Organizations (IO), identified by the United States Department of State, to verify individuals enrolled in MPP whose proceedings under section 1229a of the Immigration and Nationality Act remain ongoing to streamline their processing into the United States. Users working for an IO will download and access CBP One™ in the same manner as all other users of CBP One™. CBP will determine whether a user can have access to International Organizations functions in CBP One™ based on the information the user inputs to create a Login.gov account. Eligible International Organizations will provide email domain names to CBP and CBP will open access to the functionality within CBP One™ to users who created Login.gov accounts using that email domain. For example, the International Organization for Migration, may give CBP their email domain as @iom.int. CBP would then allow any user who created a Login.gov account using a @iom.int email to view the International Organization functionalities.

Once a user has access to the International Organization functionality in CBP One™, he or she will be able to use the application to facilitate processing of individuals that are enrolled in Migrant Protection Protocols and have an active immigration proceeding (i.e., no final adjudication). To do this, an IO user, with the consent of and on behalf of the individual, will take or upload an existing photograph of the individual into CBP One™. Once the user submits the information, CBP One™ will attempt to match the image against a pre-staged Traveler Verification Service (TVS)[54] gallery that is populated with all the images from the Migrant Protection Protocols Enforcement Integrated Database. If a match is made, CBP will send the biographic information (e.g., first and last name, date of birth) associated with the Enforcement Integrated Database image to the U.S. Citizenship and Immigration Services' Person Centric Query System (PCQS)[55] to verify that the individual still has a pending case before an immigration

---

ASSESSMENT FOR UNIFIED SECONDARY, DHS/CBP/PIA-067 (2021), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

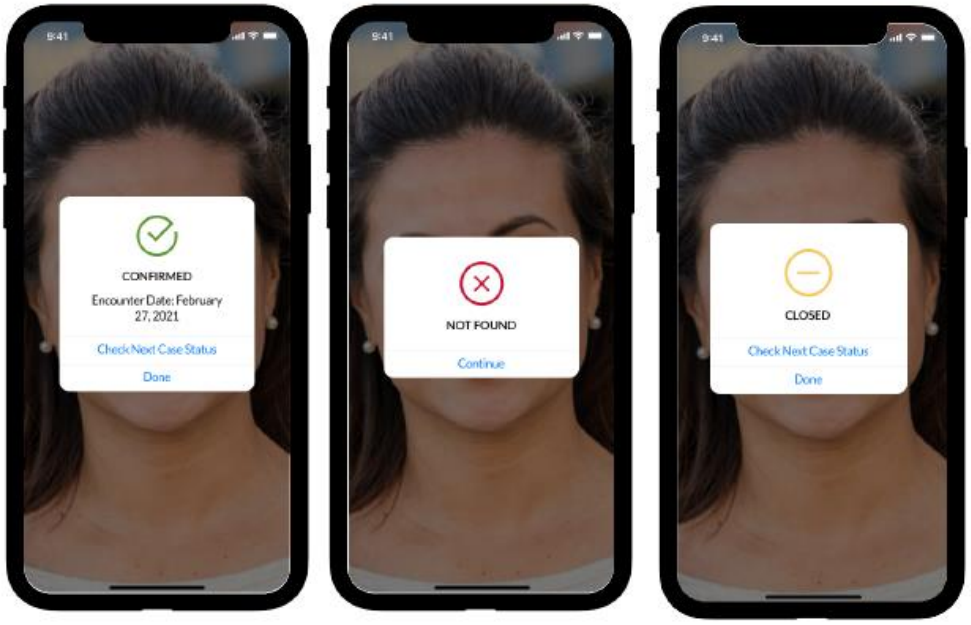
[52] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCE/IDENT, DHS/CBP/PIA-012 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[53] The Enforcement Integrated Database is a U.S. Immigration and Customs Enforcement (ICE) system that stores some CBP encounter information. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[54] *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.

[55] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010 (2016 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

judge. Individuals with a final immigration adjudication are not eligible to continue Migrant Protection Protocols processing. Once both the Enforcement Integrated Database and Person Centric Query System search are complete, CBP sends a response back to the International Organization CBP One™ user which is either a green check mark, a yellow bar, or a red "X". Additionally, the user may receive a system error message.



A green check mark indicates that the individual, whose picture the user submitted to CBP, is enrolled in Migrant Protection Protocols and has a pending case before an immigration judge. A yellow bar indicates that the individual is enrolled in Migrant Protection Protocols, but the individual's immigration case is now closed, which makes them ineligible for processing into the United States as a Migrant Protection Protocols enrollee or that CBP was unable to locate an immigration case for the individual. The International Organization can then check the U.S. Department of Justice's Executive Office for Immigration Review website to determine the case status and if the information CBP provided through CBP One™ is accurate. A red "X" means that CBP was unable to locate Migrant Protection Protocols enrollee information in CBP's Migrant Protection Protocols database in the Enforcement Integrated Database.

If they receive a red "X" the International Organization can submit an alien identification number (A-number) as an alternative method of search. Additionally, the International Organization user can select a "decline to provide" button when asked to provide a photograph of the individual which will allow the International Organization user to submit the individual's A-number, with consent of the individual. The A-number query will be sent to the Enforcement Integrated Database and Person Centric Query System to try and locate information in those

systems associated with the A-number. Like with the photograph submission, based on the record located CBP then sends a response back to the International Organization CBP One™ user with either a green check mark, yellow bar, or a red "X". If the International Organization receives another red "X", the final option will be to collect biographic information (e.g., first and last name, and date of birth) from the individual using CBP One™.[56] The biographic information is also submitted to EID and PCQS to locate matching records. As with the previous queries, CBP then sends a response back to the IO CBP One™ user with either a green check mark, a yellow bar, or a red "X". Along with the green check mark CBP will also provide the date the individual was enrolled in Migrant Protection Protocols. This will assist the International Organization in prioritizing Migrant Protection Protocols enrollees to present to CBP for processing into the United States.

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

CBP published a separate programmatic Migrant Protection Protocols Privacy Impact Assessment that discusses the privacy risks and mitigations surrounding all aspects of the program, including this use of CBP One™.[57]

2. Advance Information for Certain Undocumented Individuals on the Land Border (submitted by Non-Governmental Organizations/International Organizations)

This process for undocumented individuals is no longer in effect due to the termination of the Title 42 Order. However, CBP is keeping reference to the functionality within this Privacy Impact Assessment for historical purposes. Information about that effort is below.

On March 20, 2020, the Department of Health and Human Services (HHS) issued an Interim Final Rule (IFR) and Order under Section 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

[56] Initially, the option to input biographic information will not be available and IOs will only be able to use facial comparison and A-number inputs. CBP plans to quickly implement the biographic input option upon roll-out of this initiative.

[57] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR PROCESSING INDIVIDUALS SUBJECT TO MIGRANT PROTECTION PROTOCOLS (MPP), DHS/CBP/PIA-070 (2021), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

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

To streamline the processing at ports of entry of certain undocumented individuals who may be determined to be excepted from the Order based on humanitarian interests, CBP will leverage the existing CBP One™ Mobile Application information collection functionality, which was initially deployed in February 2021 to verify the identity and eligibility of individuals enrolled in the Migrant Protection Protocols program. Currently, CBP officers spend significant time collecting and verifying basic biographic data about undocumented individuals during the inspection process. CBP officers interview and collect information from individuals one at a time during secondary inspection. The CBP officers manually enter the information into the Unified Secondary system (USEC).[58] To facilitate processing upon arrival and reduce the amount of manual data entry into secondary processing systems, CBP One™ data will be available for importation into secondary processing events.

CBP is updating CBP One™ to allow International Organizations and now Non-Governmental Organizations (NGOs), on behalf of an undocumented individual, to submit information to CBP in advance of the individual's arrival at a port of entry. The ability to submit advance information is available to the same International Organizations and through the same process as outlined above in the Migrant Protection Protocols section of this appendix. CBP will also authenticate Non-Governmental Organizations to access the International Organization/Non-Governmental Organization functionality. DHS will inform CBP of eligible Non-Governmental Organizations based on a Non-Governmental Organization's existing roles providing services to undocumented individuals. Instead of selecting "check case status," users will select "Submit Advance Information" to collect and submit information from undocumented individuals before they arrive at a port of entry.

[58] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR UNIFIED SECONDARY, DHS/CBP/PIA-067 (2020), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection

Undocumented individuals may voluntarily provide basic biographic information name, date of birth, country of citizenship, contact information, addresses, nationality, employment history, travel history, emergency contact information, familial information, marital status, non-Western Hemisphere Travel Initiative (WHTI) compliant document information,[59] gender, preferred language, as well as an optional picture to serve as a biometric. Once an International Organization/Non-Governmental Organization has input all of the required information and any optional data fields, they will submit it to CBP. While no information is stored locally in the CBP One™ Mobile Application or on a user's device, this data is stored in a segregated backend database within the Automated Targeting System (ATS). The information will be tagged as coming from CBP One™. Additionally, CBP will store a templatized copy of the picture in a standalone Traveler Verification Service (TVS) gallery to be matched against a photograph taken by a CBP officer once the individual arrives at the port of entry using the primary inspection system. The TVS gallery will be built off the new backend dataset ingesting into the Automated Targeting System specifically for the non- Migrant Protection Protocols population. If any photos are submitted from CBP One™, the new Traveler Verification Service gallery will stage those photos until they arrive at the port of entry. CBP discusses this process in the Traveler Verification Service Privacy Impact Assessment.

Once an undocumented individual arrives at the port of entry, CBP will take a new photograph to search against the new non-Migrant Protection Protocols gallery within the Traveler Verification Service. If not found, CBP officers will manually query the Automated Targeting System based on biographic data to populate simplified arrival for processing in Primary inspection. As with any individual who arrives at the port of entry without documentation, the CBP officer will create a referral to Secondary inspection for further processing, which will include the confirmation number received from CBP One™. Once an undocumented individual is referred to Secondary, CBP will auto-populate information into the Unified Secondary system using the information captured through CBP One™. This will limit the amount of data that needs to be collected, either in Primary or in Secondary. In Secondary inspection, the officers will query the USEC event, review the accuracy of the data, edit the data as necessary to ensure accuracy, and save the information in the system. CBP is publishing an update to the Unified Secondary Privacy Impact Assessment to provide additional transparency to the process.

[59] WHTI is the joint DHS and Department of State (DOS) initiative to implement a key 9/11 Commission recommendation and the statutory mandates of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which required 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. For more information, *see* https://www.cbp.gov/travel/us-citizens/western-hemisphere-travel-initiative.

APPENDIX D: Department of Homeland Security

Updated July 25, 2024

Transportation Security Administration (TSA)

Migrant Protection Protocol Identity Verification for Domestic Flights

2024

DHS first sought to terminate the Migrant Protection Protocols (MPP) program in a June 2021 memorandum. In August 2021 the U.S. District Court for the Northern District of Texas enjoined the program termination in *Texas v. Biden*, No. 2:21-cv-067, 2021 WL 3603341 (N.D. Tex. Aug. 13, 2021). DHS terminated the program in a subsequent October 2021 memorandum that superseded the June 2021 memorandum and directed that termination be implemented as soon as practicable after a final judicial decision to vacate the *Texas* injunction. The District Court vacated the *Texas* injunction in August 2022, following a related U.S. Supreme Court ruling, and in December 2022, the District Court issued a decision staying the Secretary's October 2021 memoranda terminating the Migrant Protection Protocols program pending final resolution of the merits of the case. The Transportation Security Administration no longer uses CBP One™ for identity verification of individuals in the Migrant Protection Protocols program but is keeping reference to the functionality within this Privacy Impact Assessment for historical purposes. Information about that effort is below.

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. As part of its efforts to secure aviation transportation, TSA verifies passenger identities to grant access to airport sterile areas.[60] The TSA employee performing Transportation Document Checker (TDC) functions typically manually verifies identity at the checkpoint by comparing the facial photograph on a passenger's identity document to the passenger's actual face and the credential's biographic information to the biographic information on the passenger's boarding pass. The Transportation Document Checker also checks the boarding pass and identity credential for authenticity. Once those steps are successfully completed, the passenger proceeds to security screening.

Individuals who are enrolled in the Migrant Processing Protocol (MPP) likely will not have a valid travel document to present to TSA for identity verification. Therefore, once Migrant Processing Protocol enrollees are admitted to the United States, they will generally be unable to board domestic flights to their various destinations.

[60] "Sterile areas" are portions of airports that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator or a foreign air carrier through the screening of persons and property (49 C.F.R. § 1540.5).

CBP has created a new user role in the CBP One™ mobile application to allow TSA supervisors the ability to take a new photograph of the Migrant Protection Protocols enrollee and, using the Traveler Verification Service (TVS)[61] facial comparison technology, match the individual seeking entry to the airport sterile area with a photograph in the existing pre-staged Migrant Protection Protocols gallery. Only TSA supervisors, using a government-issued device, will be permitted to access CBP One™ for this purpose. These TSA supervisors must create an account with Login.gov using their TSA email addresses to access the TSA user role in CBP One™. TSA employees will not have access to any other CBP One™ capabilities and users that do not use the TSA email domain will not see the TSA persona on CBP One™.

As part of their ongoing assistance to Migrant Protection Protocols enrollees, International Organizations (IO) will provide information regarding further travel within the domestic United States, often in coordination with domestic aid groups. The International Organizations are responsible for communicating to the Migrant Protection Protocols enrollees that they must inform the TSA Transportation Document Checker that they lack valid travel documents but are part of the Migrant Protection Protocols. The TSA Transportation Document Checker will then refer the traveler to a TSA supervisor. The TSA supervisor will take a photograph of the traveler via his or her government-issued mobile device using the CBP One™ mobile application. CBP One™ will attempt to match the image against a pre-staged Traveler Verification Service gallery that is populated with all of the images from the Migrant Protection Protocols Enforcement Integrated Database.[62] This is the same database used for the International Organization CBP One™ functionality.[63]

If a match is made, CBP One™ will return a green check mark with the First Name, Last Name, Date of Birth, and Alien Number (A-Number) of the traveler. This will indicate that the traveler is enrolled in Migrant Protection Protocols and the TSA supervisor can check the biographic information against the traveler's boarding pass. CBP One™ will return a red "X" if no match is found.

In the event of a "no match" or if the traveler declines to be photographed, the TSA supervisor can input biographic information of the traveler which CBP One™ will attempt to match against CBP's I-94 database.[64] CBP tags Migrant Protection Protocols enrollees and

[61] *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.
[62] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[63] The MPP process will be more fully explained in a forthcoming CBP Migrant Protection Protocol PIA.
[64] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT

qualified family members[65] in the I-94 database and uses biographic information to search the database and locate enrollees and qualified family members. Just as in the biometric search, the biographic I-94 search will return a green check mark or red "X" to the TSA employee through CBP One™. If the TSA supervisor gets a red "X," they may contact the CBP Traveler Communications Center to determine if the traveler is a Migrant Protection Protocols enrollee or if the traveler should not be permitted to continue through the screening process.

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

Transportation Security Administration (TSA) at Security Checkpoints

Transportation Security Administration's (TSA) mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. As part of its efforts to secure aviation transportation, TSA is required to verify passenger identities in order to grant access to airport sterile areas.[66] The TSA employee performing Transportation Document Checker (TDC) functions typically manually verifies identity at the checkpoint by comparing the facial photograph on a passenger's identity document to the passenger's actual face and the credential's biographic information to the biographic information on the passenger's boarding pass. The TSA Transportation Document Checker also checks the boarding pass and identity credential for authenticity. Once those steps are successfully completed, the passenger proceeds to security screening.

Undocumented noncitizens may not have a valid travel document to present to TSA for identity verification. If such individuals are not in DHS custody and permitted to travel domestically, they will potentially be subject to lengthy verification processes prior to boarding domestic flights to travel to various destinations. TSA employees can only use the DHS persona in the CBP One™ application to take a photograph of certain undocumented noncitizens who lack valid travel documents and, using CBP Traveler Verification Service facial comparison

---

ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION, DHS/CBP/PIA-024(c) (2020), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[65] Qualified family members are children or spouses of an MPP enrollee who were not enrolled in MPP because they were not born or married at the time of enrollment. CBP makes this determination and tags the information in I-94.

[66] "Sterile areas" are portions of airports that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator or a foreign air carrier through the screening of persons and property (49 C.F.R. § 1540.5).

technology, match the individual seeking entry to the airport sterile area with a photograph in CBP holdings. The new photograph is matched against images in the Seizure and Arrest Workflow within the Automated Targeting System (ATS). CBP creates galleries within the Traveler Verification Service using the images of certain undocumented noncitizens located in the Seizure and Arrest Workflow. The pictures taken by TSA employees of undocumented noncitizens are matched against these galleries for identity verification purposes only.

Only TSA employees using a government-issued device will be permitted to access CBP One™ for this purpose. TSA employees utilizing their official TSA email domain will see a single persona for DHS, which will allow them to utilize CBP One™ to verify the identity of the undocumented noncitizen. TSA employees must create an account with Login.gov using their TSA email address to access to the DHS persona in CBP One™. TSA employees will not have access to any other CBP One™ capabilities, and employees that do not use the TSA email domain will not see the DHS persona on CBP One™.

When a TSA Transportation Document Checker determines that a traveler does not have valid identification, they refer the traveler to a supervisor to conduct the appropriate vetting and whether the traveler should be permitted to enter the sterile area. Depending on the traveler's interaction with the TSA supervisor and the documents they have available, a TSA supervisor may decide to use CBP One™ to retrieve the traveler's identity in CBP holdings. The TSA supervisor will take a photograph of the traveler via his or her government-issued mobile device or laptop using the CBP One™ application. CBP One™ uses the Traveler Verification Service to templatize and match the live facial photograph captured from the undocumented noncitizen against a facial photograph from a staged gallery that is populated with images from the Automated Targeting System database. If a match is made, CBP One™ will return a green check mark with the First Name, Last Name, Date of Birth, A-Number (if available), citizenship of the traveler, and a facial photograph of the traveler (if available). The TSA employee can then check the travelers biographic and biometric information displayed on CBP One™ against the traveler's boarding pass.

CBP One™ will return a red "X" if no match is found. In the event of a "no match" , the TSA user can search CBP One™ by the traveler's biographic information or A-Number. CBP One™ will attempt to match the biographic data or A-Number entered into the mobile application against the Automated Targeting System database. The biographic or A-Number search will return either a green check mark or red "X" to the TSA user through CBP One™. If the TSA user gets a red "X," they can contact their National Transportation Vetting Center to determine if the traveler should not be permitted to continue through the screening process.

As with other CBP One™ uses, no information is stored locally on the device. CBP does not store the photo but will store the A-Number and biographic data, if provided, in a CBP Amazon

Web Services Cloud Service (CACE) database for 365 days. This data will be retrievable by CBP employees in the CBP Office of Information Technology to provide CBP leadership with anonymized statistics related to workload and record location ability. For example, CBP or TSA supervisors will be able to obtain aggregate data (*e.g.*, number of submissions); no information is stored as part of this process.

APPENDIX E: Carriers and Operators

Updated July 25, 2024

Advance Manifest Information from Bus Carriers and/or Bus Companies

In December 2019, CBP published the Advance Passenger Information System (APIS): Land Pre-Arrival System (LPAS) for Bus and Rail Privacy Impact Assessment Update, which discussed the new Land Pre-Arrival System functionality, embedded into the CBP Reporting Offsite Arrival – Mobile (ROAM)™ application.[67] The Land Pre-Arrival System functionality provided bus and rail carriers, entering the United States, a mobile option to submit an Advance Passenger Information System manifest and carrier information to CBP prior to crossing a U.S. land border. In August 2021, the Land Pre-Arrival System bus manifest functionality migrated to the CBP One™ mobile application. The Land Pre-Arrival System bus manifest functionality is no longer available through CBP Reporting Offsite Arrival – Mobile (ROAM)™. The rail manifest functionality remains in Reporting Offsite Arrival – Mobile (ROAM)™ and there are no current plans to migrate this functionality to CBP One™.

Bus carriers and/or the bus companies (referred to below as users) can now use CBP One™ to voluntarily submit their bus manifest information to CBP prior to arriving at a land port of entry. Once the user has logged in via Login.gov and consented to the privacy policy, the landing page will launch which permits the user to select from different options that describe the individual's reason for using CBP One™. To access this functionality in CBP One™, the user must select the "bus operator" option (or "persona") from the landing page.

Once the user accesses the bus operator persona, they will be prompted to enter their assigned carrier code and sender ID.[68] The carrier code and sender ID are an additional layer of security used to authenticate the bus carrier employee into the bus operator user profile. These two fields only appear when the user logs into the bus operator option from the landing page. Without the carrier code and sender ID, the bus carrier employee cannot access the bus operator portion of the app. The operator will then be required to enter the conveyance registration number, status of registration, and operator's company name.

After the user is authenticated through CBP One™, they will be directed to provide their bus manifest data. The operator will be required to provide the arrival location in the United States; departure date of trip; departure time of trip; arrival date to the United States; arrival time to the

[67] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCED INFORMATION SYSTEM (APIS): LAND PRE-ARRIVAL SYSTEM (LPAS) FOR BUS AND RAIL, DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[68] CBP issues both the carrier code and sender ID to bus carriers. Both codes are unique identifiers and are used to identify the bus carrier company in the Advance Passenger Information System.

U.S. port of entry; port of entry arriving to; last country visited; and contact email/phone number for bus operator.

The user is then prompted to manually provide passenger biographic and trip information into the submission screen. Alternatively, the user can use their phone camera to scan the passengers' Western Hemisphere Travel Initiative (WHTI)-compliant document with a Machine Readable Zone (MRZ) to populate the biographic information into the travel document text fields of the submission screen. The following biographic data will be collected from the passenger through CBP One™: first and last name; date of birth; gender; country of citizenship; country of residence; document type; document number; date of issue; date of expiration; country of issue; and Trusted Traveler number (if a Trusted Traveler document was presented). Once the user has scanned the Machine Readable Zone of all passengers' Western Hemisphere Travel Initiative compliance document or manually entered their biographic information (if necessary) into CBP One™, they will be prompted to submit the manifest to CBP. The photo on the travel document will be collected during the Machine Readable Zone scan. However, the image is deleted upon submission to CBP and is not viewed or used by CBP officers.

Once the data is submitted through CBP One™, law enforcement checks are completed via the TECS[69] and an Advance Passenger Information System manifest is created. CBP officers will then review the manifest and conduct enhanced checks as needed. In addition, CBP officers use the information submitted through CBP One™ to conduct targeting queries and review passengers in advance of their arrival at the land border. Once a passenger arrives at the port of entry, officers will utilize Simplified Arrival (SA)[70] or mobile primary to process the passenger and match them to the data submitted to the Advance Passenger Information System through CBP One™.

The carrier code and sender ID collected from the bus driver and submitted through the bus operator persona is sent to CBP Advance Passenger Information System and will be written into the Advance Passenger Information System manifest. This happens at the time of submission. Additionally, at the time of submission, the carrier code and sender ID are immediately erased from CBP One™. All trip and biographic data collected from the bus driver and passengers through the user's mobile device will be deleted after submission to CBP, or after 24 hours from collection.

---

[69] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: CBP PRIMARY AND SECONDARY PROCESSING, DHS/CBP/PIA-009 (2010 and subsequent updates), and U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[70] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

All data, except for the mobile device information discussed below, submitted through CBP One™ will be forwarded immediately to the Advance Passenger Information System and will not be retained in the CBP One™ Amazon Web Services cloud. Advance Passenger Information System data is used for entry screening purposes and is retained for 13 months. Furthermore, while the Advance Passenger Information System only retains information for a limited period of time, all or a portion of Advance Passenger Information System data is immediately transmitted to the Automated Targeting System (ATS),[71] TECS, and the Arrival and Departure Information System (ADIS)[72] upon receipt. Advance Passenger Information System information is ingested into the following systems and stored according to their respective retention schedules: the Automated Targeting System (15 years), Arrival and Departure Information System (75 years), and TECS (75 years). All mobile device information collected (e.g., Device Type, Device ID, Operating System Version, and Phone Model) is retained for 365 days in the CBP Amazon Web Services Cloud Service (CACE) database.

[71] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006(e) (2022), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[72] *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.

APPENDIX F: Other CBP One Use Cases

Updated July 25, 2024

Undocumented individuals located in Mexico are currently the only eligible population who can request an appointment via CBP One™. As part of its efforts to manage migration within Mexico, Mexico has requested that the National Institute of Migration, an agency of the government of Mexico, have a mechanism to validate that an individual they encounter has a valid CBP One™ appointment. To respond to this request, CBP created the CBP One™ Appointment Validation Tool. The Appointment Validation Tool is the only CBP One™ capability available to National Institute of Migration users with a valid National Institute of Migration email domain and with a need to know. This tool does not share personally identifiable information with the National Institute of Migration, though it does confirm whether the date of birth/appointment confirmation number input into the tool are information maintained by CBP and whether an individual (or group of individuals) has an existing appointment with CBP.

CBP intends to share this limited information with certain National Institute of Migration users to support their encounters with undocumented individuals located in Mexico. While Mexico maintains its own authorities with respect to migration and individuals encountered, CBP is sharing this information to indicate to National Institute of Migration personnel which individuals may already have an appointment with CBP and which individuals may need to schedule an appointment with CBP if they intend to reach the United States. This sharing is not intended to inform a negative inference by National Institute of Migration users about the individuals they may encounter.

National Institute of Migration employees can download CBP One™ from the Google Play or iTunes mobile application stores. National Institute of Migration users will be prompted to create a new Login.gov account or login to an existing Login.gov account. Personnel must use their official National Institute of Migration email address to access CBP One™.[73] When users log into CBP One™; users must consent to the CBP Privacy Policy[74] before using the application.

Inside of CBP One™, National Institute of Migration personnel will be presented with only one option: "Check Traveler Appointment." The National Institute of Migration personnel cannot utilize CBP One™ for any other reason under their official National Institute of Migration email Login.gov account. The National Institute of Migration user will input a CBP One™ appointment

[73] 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.

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

confirmation number and traveler's date of birth based on information the traveler provides to National Institute of Migration personnel during their encounter. Once the National Institute of Migration user initiates a search, the CBP One™ application will query the CBP Amazon Web Services Cloud Service (CACE) to locate a registration. If the app locates a matching registration with a confirmed future appointment, the application will display the appointment date, time, location, and the total number of travelers in the registration. If the traveler does not have a confirmed appointment, the app will display a red "X" and "No Appointment Found." CBP does not conduct any system checks other than to verify the existence of a traveler's appointment. CBP will store the National Institute of Migration query for one year within the CBP Amazon Web Services Cloud East environment. This information is stored for reporting purposes only.