Privacy Impact Assessment

for the

CBP One™ Mobile Application

DHS Reference No. DHS/CBP/PIA-068

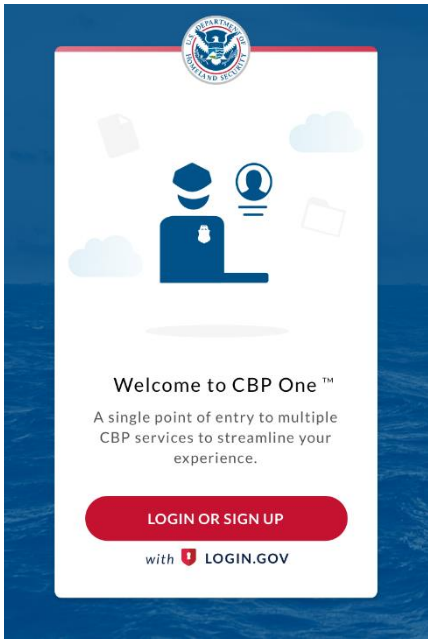
February 19, 2021

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), launched a new public-facing mobile application, CBP One™, to provide the public a single portal to a variety of CBP services. 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™ mobile application. CBP One™ is a mobile 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.


Welcome to CBP One ™

A single point of entry to multiple CBP services to streamline your experience.

Figure 1: CBP One Login Screen

CBP One™ is available for Android and iOS mobile devices in the Google Play or iTunes mobile application stores. Users have to 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. In order to register with Login.gov, users have to provide an email address and a phone number and create a password. Login.gov does not share any information provided by the user with CBP. Each time a user launches CBP One™, a notification displaying the CBP Privacy Policy will appear and users must consent to it prior to using the mobile application.

Once the user has logged in via Login.gov and consented to the privacy policy, the landing page will launch which permits the user to select from different options that describe the individual's 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 Spring 2021, 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 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.

[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 PIA, International Organizations have established roles supporting the Government of Mexico to provide services to undocumented individuals under the Migrant Protections Protocol (MPP).

[3] The MPP 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.

Also by Spring 2021, 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. 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 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

[5] 5 U.S.C. § 552a.
[6] 6 U.S.C. § 142(a)(2).
[7] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY

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.

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

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, *available at* https://www.cbp.gov/about/mobile-apps-directory/cbpone.

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™ to verify their enrollment in MPP.

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).

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.

[11] *See* DHS/CBP-001 Import Information System, 81 FR 48826 (July 26, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

[12] *See* DHS/CBP-007 Border Crossing Information (BCI), 81 FR 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 FR 72081 (November 18, 2015), *available at* https://www.dhs.gov/system-records-notices-sorns.

[14] *See* DHS/CBP-006 Automated Targeting System (ATS), 80 FR 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 FR 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 FR 77778 (December 19, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

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.

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

[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.

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

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 PIA that discusses the SRME function in more detail and also update the existing I-94 PIA series to include the CBP One™ mobile application as a way in which individuals can apply for and check their I-94s.

Reporting Offsite Arrival-Mobile (ROAM)

The ROAM mobile 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 ROAM 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 PIA to discuss the privacy risks and mitigations thoroughly. CBP will update this Appendix when the standalone PIA is published.

APPENDIX B: Importers/Exporters

Stakeholder Scheduling

The Stakeholder Scheduling functionality is embedded into the CBP One™ mobile application, and provides brokers, importers, and travelers the option to voluntarily schedule inspection appointments and assist in the management of appointments related to CBP cargo services.

APPENDIX C: Non-Governmental Organizations

Migrant Protection Protocol

In early 2019, CBP began implementing the Migrant Protection Protocol (MPP),[18] which is a U.S. government action whereby certain foreign individuals, without proper documentation, entering or seeking admission to the United States from Mexico are returned to Mexico to wait outside of the United States for the duration of their immigration proceedings. In January 2021,[19] the United States ended new enrollments into MPP and, in February 2021, began the process of permitting foreign individuals previously in MPP to be processed into the United States. In order to enroll individuals in MPP, CBP used Unified Secondary[20] and e3[21] to collect a photograph and biographic information from the individual. CBP stores this information in a CBP database in the Enforcement Integrated Database (EID).[22]

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 IO functions in CBP One™ based on the information the user inputs to create a Login.gov account. Eligible IOs 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, a designated IO, 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 IO functionalities.

[18] *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.

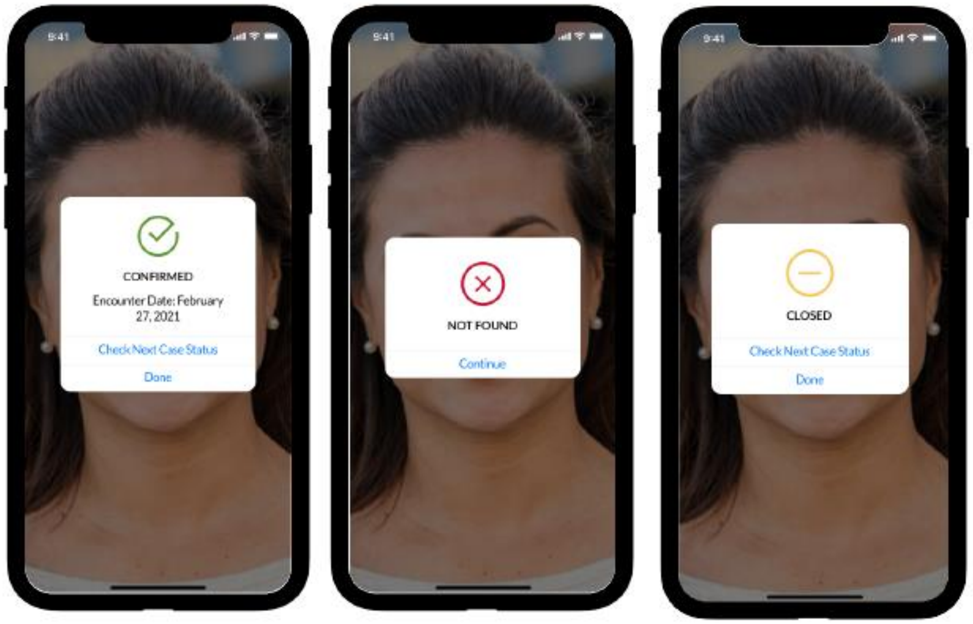
[19] *See* Executive Order 14010, Creating a Comprehensive Regional Framework To Address the Causes of Migration, To Manage Migration Throughout North and Central America, and To Provide Safe and Orderly Processing of Asylum Seekers at the United States Border (February 3, 2021), *available at* https://www.federalregister.gov/presidential-documents/executive-ord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

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

[21] *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.

[22] EID 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.

Once a user has access to the IO functionality in CBP One™, he or she will be able to use the application to facilitate processing of individuals that are enrolled in MPP 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)[23] gallery that is populated with all of the images from the MPP EID database. If a match is made, CBP will send the biographic information (e.g., first and last name, date of birth) associated with the EID image to the U.S. Citizenship and Immigration Services' Person Centric Query System (PCQS)[24] to verify that the individual still has a pending case before an immigration judge. Individuals with a final immigration adjudication are not eligible to continue MPP processing. Once both the EID and PCQS search are complete, CBP sends a response back to the IO 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.



CONFIRMED

Encounter Date: February 27, 2021

NOT FOUND

CLOSED

A green check mark indicates that the individual, whose picture the user submitted to CBP, is enrolled in MPP and has a pending case before an immigration judge. A yellow bar indicates that the individual is enrolled in MPP, but the individual's immigration case is now closed, which makes them ineligible for processing into the United States as an MPP enrollee or that CBP was

[23] *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.

[24] *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.

unable to locate an immigration case for the individual. The IO 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 MPP enrollee information in CBP's MPP database in EID.

If they receive a red "X" the IO can submit an alien identification number (A-number) as an alternative method of search. Additionally, the IO user can select a "decline to provide" button when asked to provide a photograph of the individual which will allow the IO user to submit the individual's A-number, with consent of the individual. The A-number query will be sent to EID and PCQS to try and locate information in those systems associated with the A-number. Like with the photograph submission, based on the record located CBP then sends a response back to the IO CBP One™ user with either a green check mark, yellow bar, or a red "X". If the IO 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™.[25] 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 MPP enrollee was enrolled in MPP. This will assist the IO in prioritizing MPP 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 in order to provide CBP leadership with anonymized statistics related to workload and record location ability. For example, CBP employees will be able to view number of submissions and number of submissions that required submitting the A-number and biographic data.

CBP is publishing a separate programmatic MPP PIA that will discuss the privacy risks and mitigations surrounding all aspects of the MPP program, including this use of CBP One™.

[25] 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.

APPENDIX D: Transportation Security Administration (TSA)

Updated February 26, 2021

Migrant Protection Protocol Identity Verification for Domestic Flights

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 verifies passenger identities in order to grant access to airport sterile areas.[26] 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 TDC 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 MPP enrollees are admitted to the United States, they will generally be unable to board domestic flights to their various destinations.

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 MPP enrollee and, using the Traveler Verification Service (TVS)[27] facial comparison technology, match the individual seeking entry to the airport sterile area with a photograph in the existing pre-staged MPP gallery. Only TSA supervisors, using a government-issued device, at certain airports near the border 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 MPP enrollees, International Organizations (IO) will provide information regarding further travel within the domestic United States, often in coordination with domestic aid groups. The IOs are responsible for communicating to the MPP enrollees that they must inform the TSA TDC that they lack valid travel documents but are part of MPP. The TSA TDC will then refer the traveler to a TSA supervisor. The TSA supervisor will,

[26] "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).

[27] *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.

with the consent of the traveler, 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 TVS gallery that is populated with all of the images from the MPP EID[28] database. This is the same database used for the IO CBP One™ functionality.[29]

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 MPP 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.[30] CBP tags MPP enrollees and qualified family members[31] in the I-94 database and uses biographic information to search the database and locate MPP 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 user through CBP One™. If the TSA supervisor gets a red "X" he or she may contact CBP Traveler Communications Center to determine if the traveler is an MPP 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 in order to provide CBP leadership with anonymized statistics related to workload and record location ability. For example, CBP employees will be able to view number of submissions and number of submissions that required submitting the A-Number and biographic data. TSA stores no information as part of this process.

[28] *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.
[29] The MPP process will be more fully explained in a forthcoming CBP Migrant Protection Protocol PIA.
[30] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT 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.
[31] 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.