



Privacy Impact Assessment

for the

CBP One™

DHS Reference No. DHS/CBP/PIA-068(a)

July 25, 2024



Homeland
Security



Abstract

CBP One™, a mobile and web application, provides the public a single portal to a variety of CBP services. CBP One™ includes different functionality for travelers, importers, brokers, carriers, international organizations, federal personnel, 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) update to clarify that CBP One™ stores information locally on a user's device.

Overview

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 \(dhs.gov\)](https://www.dhs.gov/cbpone). Users must create a new or open an existing Login.Gov¹ account to access CBP One™. Login.Gov ensures a secure connection and identity verification for CBP One™ users. To register with Login.gov, users must provide an e-mail 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 Policy² will appear, and users must consent to it prior to using the 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 may input information for themselves and others (e.g., co-travelers, family members). This makes it easier for groups to submit information and streamlines CBP's vetting and inspection processes.

Currently, CBP One™ is available for functionality for travelers, importers, brokers, carriers, international organizations, federal personnel, and other entities. Each functionality and use case is fully described in appendices to this Privacy Impact Assessment series. As users and functionalities are added, CBP will continue updating the Privacy Impact Assessment and/or appendix for this Privacy Impact Assessment series.

Reason for the PIA Update

DHS/CBP/PIA-068 CBP One™ stated that regardless of the function, CBP One™ does

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>.

² The CBP One™ Privacy Policy can be found at <https://cbpone.cbp.dhs.gov/#/>.



not store any information locally on the device or within the CBP One™ application itself. CBP pushes all information collected through CBP One™ to back-end systems associated with the functions the user is using. For example, CBP stores information related to I-94 information submitted through CBP One™ in CBP's I-94 databases, not in the mobile or web application.

While it is accurate that CBP pushes all information collected through CBP One™ to back-end systems associated with the functions the user is using, CBP is issuing this Privacy Impact Assessment Update to clarify the retention statement previously made in the DHS/CBP/PIA-068 CBP One™ Privacy Impact Assessment.

The previous Privacy Impact Assessment stated that no information is stored locally on the user's device or in the CBP One™ application itself. However, to use the application, CBP One™ users are required to create a user profile. To create a user profile, the CBP One™ application collects and stores the first and last name of the user. Once a user profile is created, this information is stored locally on the user's device (for the mobile application submissions) and in local web storage (for the website application). The local storage enables users to quickly retrieve information submitted through the application for subsequent use. No other biographic information is collected or stored locally on the mobile device or in web storage. No biometric information is collected as part of the user profile or stored locally on the mobile device or in web storage.

Additionally, as part of the Login.gov process, Login.gov sends the e-mail address used to create the user profile to CBP for access and storage. CBP stores the e-mail address in the CBP Amazon Web Services Cloud East for one year for reporting and auditing purposes.

Privacy Impact Analysis

Authorities and Other Requirements

There are no changes to CBP authorities and other requirements to operate the CBP One™ application with this Privacy Impact Assessment update.

Characterization of the Information

There are no changes to the collection of information with this Privacy Impact Assessment update. CBP is issuing this Privacy Impact Assessment update to clarify that limited user information is collected and stored locally on either the user's mobile device or web storage. The user profile information is a subset of information that is already collected through the CBP One™ application (i.e., first and last name). A user can modify or update their user profile information at any time.

Additionally, consistent with Login.gov standard operating procedures, the e-mail address used to create the Login.gov account is sent to CBP for access and storage. This information was inaccurately described previously as not being stored. CBP does not have access to nor does it use



the password or authentication methods used to log into the mobile application as this is managed through Login.gov.

Uses of the Information

This update does not impact the use of information. CBP One™ allows users to interact with CBP for a variety of purposes; therefore, the information provided to CBP via CBP One™ is also used for a variety of purposes. The user's first and last name is collected as part of the user profile creation. This information is stored locally on the mobile device or within web storage to create a user profile within CBP One™ so that the user can quickly retrieve information for subsequent uses. This information is not accessed or used by CBP. CBP does not have access to any user profile information that is stored locally.

Additionally, consistent with Login.gov standard operating procedures, the e-mail address used to create the Login.gov account is sent to CBP for access and storage. The e-mail address is also collected as part of the biographic information that is typically collected during the function-specific CBP One™ process and may be used for a specific CBP One™ use case (e.g., to provide an e-mail confirmation to a traveler who registered for an appointment at a port of entry).

Notice

CBP is providing notice of these changes through the publication of this Privacy Impact Assessment update.

Data Retention by the Project

CBP One™ collects and stores the first and last name of the user as part of the profile creation. This information is stored locally on the mobile device or within web storage to create a user profile within CBP One™ so that the user can quickly retrieve information for subsequent uses. No other biographic information is stored on the mobile device or within the web storage. The user profile information is stored locally until the user chooses to delete the application.

Additionally, consistent with Login.gov standard operating procedures, the e-mail address used to create the Login.gov account is sent to CBP for access and storage. CBP stores the e-mail address in the CBP Amazon Web Services Cloud East for one year for reporting and auditing purposes.

Information Sharing

There are no changes to information sharing because of this update.

Redress

This update does not impact how access, redress, and correction may be sought through CBP.



Auditing and Accountability

There are no changes to auditing and accountability because of this update.

Contact Official

Jody Hardin
Executive Director
Planning, Program Analysis and Evaluation
Office of Field Operations
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection
privacy.cbp@cbp.dhs.gov

Approval Signature

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

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
privacy@hq.dhs.gov