Privacy Impact Assessment

for the

CBP Link

DHS Reference No. DHS/CBP/PIA-083

June 11, 2025

Homeland Security

Abstract

1. The abstract is the single paragraph that will be used to describe the program and the Privacy Impact Assessment.[1]
The U.S. Department of Homeland Security, U.S. Customs and Border Protection (CBP), has launched a public-facing application called CBP Link, previously named CBP One™.[2] This application provides a single portal for the public to access a variety of services and is available as both a mobile and web application. CBP Link offers different functionalities for various groups, including members of the public, brokers, carriers, operators, and U.S. Department of Homeland Security personnel, all under a single consolidated log-in. The application uses guided questions to help users determine the correct services, forms, or applications needed to interact with the U.S. Customs and Border Protection. The U.S. Customs and Border Protection is conducting this Privacy Impact Assessment to address privacy risks associated with the collection, maintenance, use, and dissemination of information through the CBP Link application.

Overview

2. The overview provides the context and background necessary to understand the project's purpose and mission and the justification for operating a privacy sensitive project.
CBP Link is a public-facing mobile and website application that provides a single portal for accessing a variety of services. It offers different functionalities for members of the public, brokers/carriers/operators, and U.S. Department of Homeland Security personnel, all under a single consolidated log-in. CBP Link uses guided questions to help users find the correct services, forms, or applications based on what they need to do. CBP Link is available for Android and iPhone Operating System (iOS) mobile devices in the

[1] Pursuant to Section 208 of the E-Government Act of 2002, agencies are required to conduct a Privacy Impact Assessment before developing or procuring Information Technology systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public. The Office of Management and Budget issued Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, which defines "information in identifiable form" as information in an Information Technology system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements. Furthermore, an individual is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence."

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP ONE™ MOBILE APPLICATION (2024), *available at* DHS/CBP/PIA-068 CBP One™ Mobile Application | Homeland Security. This Privacy Impact Assessment will be retired upon publication of CBP Link.

Google or Apple mobile application stores, as well as on the web. Users must create a new or use an existing Login.gov[3] account to access CBP Link. Login.gov ensures a secure connection and verifies the identity of CBP Link users. To register with Login.gov, users need to provide an email address, a phone number, and create a password. Login.gov does not share any user information with the U.S. Customs and Border Protection. Each time a user opens CBP Link, a notification displaying the Terms and Conditions, including the privacy policy, will appear. Users must accept these Terms and Conditions before using the application.

Once the user has logged in through Login.gov and accepted the privacy policy, the CBP Link landing page will open, allowing users to choose from different options that help determine the appropriate functions based on their reason for using CBP Link. These functions include access to the following services, based on the type of persona:

Traveler Persona

I-94 Mobile[4]

This functionality is primarily for individuals issued a Form I-94, which may include individuals who have become naturalized U.S. citizens or Lawful Permanent Residents (LPRs). I-94 Mobile is a function of CBP Link and offers the same features as the current U.S. Customs and Border Protection I-94 website[5] (such as retrieving 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 of capturing 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. U.S. citizens and Lawful Permanent Residents are generally unable to use CBP Link to look up information about themselves, however, their historic travel records are available for the period before they are naturalized or receive Lawful Permanent Resident status.[6]

Voluntary Self-Reported Exit

The CBP Link Voluntary Self-Reported Exit functionality provides a mobile option for eligible aliens who have been issued an I-94 to voluntarily self-report their own (and any co-travelers)

[3] *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.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE I-94 WEBSITE APPLICATION), DHS/CBP/PIA-016 (2013 and subsequent updates), *available at* Privacy Documents for CBP | Homeland Security.

[5] *See* Official Site for Travelers Visiting the United States (March 2025), *available at* https://i94.cbp.dhs.gov/home.

[6] The Arrival and Departure Information System (ADIS) is the backend system for U.S. Customs and Border Protection I-94 data, which includes the travel history of all travelers, including U.S. citizens and Lawful Permanent Residents. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, *See* U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE SYSTEM, DHS/CBP/PIA-024 (2020), *available at* Privacy Documents for CBP | Homeland Security.

exit from the United States. Co-travelers may include U.S. citizens and Lawful Permanent Residents, especially minor children or dependents. First, eligible aliens and co-travelers (collectively referred to as "users") use the mobile application to perform a one-time geolocation ping to ensure the mobile device the user is using to report is outside of the United States. Geolocation permits U.S. Customs and Border Protection to determine the accuracy of the location reported by the user, to identify fraudulent uses of the Voluntary Self-Reported Exit functionality, and to detect "spoofing" techniques that may alter the location of the mobile device (e.g., the mobile device user is not within the Voluntary Self-Reported Exit radius requirement of at least three miles beyond the U.S. border).[7] If the mobile device's geolocation is confirmed to be outside the United States, the user will be permitted to continue to the next step in the process.

CBP Link will then prompt the user to allow access to their mobile device's camera, and a consent notification will appear. U.S. Customs and Border Protection uses the camera on the mobile device to read the "Machine-Readable Zone" of a passport, or other authorized travel document and to take a "selfie" of the user.[8] If the user declines the camera consent notification, he or she cannot proceed further through the Voluntary Self-Reported Exit functionality. Users who are unable or unwilling to use CBP Link to voluntarily report their exit are still encouraged to report their exit by traditional options.[9]

To scan their travel document, the user selects "Scan Passport", which uses the mobile device's camera to scan the travel document, including the "Machine-Readable Zone" on the travel document.[10] The machine-readable scan collects the following information from the travel document: name, date of birth, sex, document identification/number, document type, and issuing country. The user is then required to select the country in which they are currently present while reporting their exit.

The next step is for the user to take a "selfie." The mobile application instructs the user to line up their face with a box and to perform a "liveness" test to determine that it is a real person (and

[7] In this context, geolocation is collected to help detect submissions of information from a non-trusted source.
[8] The Machine-Readable Zone is the alphanumerical lines on a travel document (e.g., passport) that is scanned and deciphered by machines.
[9] Aliens may report their exit in the following ways: 1) to a U.S. Customs and Border Protection officer at a port of entry, who will in turn, update the Arrival and Departure Information System; 2) drop a copy of their paper U.S. Customs and Border Protection I-94 (if applicable) in a drop box at a port of entry before exiting the United States; or 3) mail a copy of their U.S. Customs and Border Protection I-94 directly to the third-party data entry service for processing.
[10] The mobile device then scans the Machine-Readable Zone of the travel document to capture and retrieve biographic information including name, travel document number, nationality, date of birth, sex, and travel document expiration date. This biographic information is then automatically populated into the mobile application to eliminate the need for the alien to manually input this information.

not a picture of a person).[11] Once complete, the mobile application takes a photograph.[12] Once successfully captured, the user can review the submission details before submission to U.S. Customs and Border Protection. After reviewing the information, the user selects "submit."

Upon submission, U.S. Customs and Border Protection uses the biographic and travel document information submitted by the user to pull a source photo from U.S. Customs and Border Protection's holdings, which contains travel document source photos (e.g., passport, border crossing card, and previous encounter images), in near real-time. U.S. Customs and Border Protection uses the Traveler Verification Service as the backend matching service to conduct a 1:1 facial comparison matching between the source photograph in U.S. Customs and Border Protection holdings and the "selfie" submitted by the user voluntarily reporting their exit.[13] If there is a match between the photographs, then the user exit is recorded as a biometrically confirmed exit in U.S. Customs and Border Protection TECS (not an acronym),[14] the Arrival and Departure Information System, and the U.S. Department of Homeland Security Automated Biometric Identification System/Homeland Advanced Recognition Technology.[15] If the Traveler Verification Service is not able to successfully match the source photograph from U.S. Customs and Border Protection holdings to the "selfie" the mobile device user will receive a

[11] A liveness test is completed to verify that a newly collected photograph is being performed by a live, genuine person, not a spoof or fake presentation. While the individual is taking the "selfie," the technology embedded within the application relies on the devices camera to view a live image through three-dimensional face changes and observing perspective distortion to prove the image is three-dimensional. If "liveness" cannot be confirmed, the user is unable to utilize the CBP Link.

[12] While the applicant is taking the "self-image," the technology embedded within the mobile application relies on the device's camera to view a live image through three-dimensional (3D) face changes and observing perspective distortion to prove the image is three-dimensional. If "liveness" cannot be confirmed, the applicant is unable to proceed with submitting their exit through the CBP Link mobile application.

[13] *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 and subsequent updates), *available at* Privacy Documents for CBP | Homeland Security.

[14] *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* Privacy Documents for CBP | Homeland Security.

[15] CBP enrolls alien travelers in the U.S. Department of Homeland Security Automated Biometric Identification System (IDENT) as a biometric confirmation of arrival and exit, when possible. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *available at* Privacy Documents for the Office of Biometric Identity Management (OBIM) | Homeland Security. U.S. Department of Homeland Security is replacing AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM with the Homeland Advanced Recognition Technology System (HART) as the primary U.S. Department of Homeland Security system for storing and processing of biometric and associated biographic information. For more information about Homeland Advanced Recognition Technology System, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020*), available at* Privacy Documents for the Office of Biometric Identity Management (OBIM) | Homeland Security.

message to "Try Again Later" or be instructed to visit https://i94.cbp.dhs.gov/ for more information on alternative ways to report their exit. If this occurs, the exit will not be recorded in any system.

If an exit is successfully submitted, CBP Link displays a confirmation message indicating that U.S. Customs and Border Protection has received their exit submission, and they can access their exit record in either CBP Link or through the I-94 website in near-real time.

Broker/Carrier/Forwarder Persona

Stakeholder Scheduling

The Stakeholder Scheduling functionality in the CBP Link application provides a mobile and web option for brokers, carriers, forwarders,[16] 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 U.S. Customs and Border Protection Agricultural Specialist within a chat feature embedded into the mobile and desktop application.

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

Scheduling Dashboard

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

[16] International freight forwarders are agents for exporters and can move cargo from "dock-to-door," providing several significant services such as arranging for and tracking of freight from a domestic and international perspective; arranging for and tracking inland transportation; preparation of shipping and export documents; warehousing; booking cargo space; negotiating freight charges; freight consolidation; cargo insurance. For additional information about customs brokers and freight forwarders, *see* https://www.trade.gov/customs-brokers-and-freight-forwarders.

U.S. Department of Homeland Security Persona

TSA Transportation Document Check Functionality

As part of its efforts to secure aviation transportation, the Transportation Security Administration is required to verify passenger identities in order to grant access to airport sterile areas.[17] The Transportation Security Administration employee performing Transportation Document Checker 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.[18] 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.

When the 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 decide whether the traveler should be permitted to enter the sterile area. Depending on the traveler's interaction with the Transportation Security Administration supervisor and the documents they have available, a Transportation Security Administration supervisor may use CBP Link to determine the traveler's identity using information in U.S. Customs and Border Protection holdings.

Upon login, Transportation Security Administration supervisory employees using their official TSA email domain will only see a single persona for U.S. Department of Homeland Security, which will allow them to use CBP Link to verify the identity of the traveler. CBP Link will prompt the Transportation Security Administration supervisor to submit a photograph of the traveler, and the CBP Link application will transmit the newly captured photograph to the U.S. Customs and Border Protection Traveler Verification Service to templatize and match against a gallery of facial images from the gallery within the U.S. Customs and Border Protection Automated Targeting System.[19] If a match is made, CBP Link will return the first name, last name, date of birth, Alien Registration Number (if available), citizenship, and matched facial

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

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVEL DOCUMENT CHECKER AUTOMATION USING FACIAL IDENTIFICATION, DHS/TSA/PIA-046 (2018 and subsequent updates), and *see* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVEL DOCUMENT CHECKER AUTOMATION – DIGITAL IDENTITY TECHNOLOGY PILOTS (2022), *available at* Privacy Documents for TSA | Homeland Security.

[19] *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 (2007 and subsequent updates), *available at* Privacy Documents for CBP | Homeland Security.

photograph (if available). CBP Link will also advise the Transportation Security Administration if the traveler presented a passport during their inspection on their most recent arrival, whether they submitted their intent to depart through CBP Link, and whether the Immigration and Customs Enforcement has determined that the traveler is eligible to fly domestically. The Transportation Security Administration employee can then check the biographic and biometric information displayed on CBP Link against the boarding pass.

CBP Link will also advise if no match to the traveler's photo is found. In the event of a "no match," the Transportation Security Administration user can search CBP Link by the traveler's biographic information or Alien Registration Number. CBP Link will attempt to match the biographic data or Alien Registration Number entered into the mobile application against the U.S. Customs and Border Protection Automated Targeting System database and U.S. Customs and Border Protection TECS. Once CBP Link locates a match to the biographic data, the U.S. Customs and Border Protection Traveler Verification Service will conduct a 1:1 comparison against the newly captured photograph and the photograph found in U.S. Customs and Border Protection TECS matched to the biographic data. If a 1:1 match is made, CBP Link will return to the first name, last name, date of birth, Alien Registration Number (if available for aliens), citizenship, and associated facial photograph. The Transportation Security Administration supervisor then checks the biographic information against the boarding pass and biometric information displayed on CBP Link against the traveler to confirm identity. If the Transportation Security Administration user gets a red "X," they can contact their National Transportation Vetting Center for further vetting.

U.S. Customs and Border Protection does not store the photograph but will store the Alien Registration Number and biographic data, if provided, for 365 days. This data is retrievable by U.S. Customs and Border Protection Office of Information Technology to provide U.S. Customs and Border Protection leadership with anonymized statistics related to workload and record location ability. For example, U.S. Customs and Border Protection or Transportation Security Administration leadership will be able to obtain aggregate data (e.g., number of submissions). No other information is stored as part of this process.

Bus Operator Persona

Advance Manifest Information

Bus carriers and/or the bus companies (referred to as "users") can now use CBP Link to voluntarily submit their bus manifest information to U.S. Customs and Border Protection prior to arriving at a land port of entry. To access this functionality in CBP Link, 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 identification.[20] The carrier code and sender identification 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 identification, the bus carrier employee cannot access the bus operator portion of the application. The operator will then be required to enter the bus registration number, status of registration, and the operator's company name.

After the user is authenticated through CBP Link, 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 the trip; departure time of the trip; arrival date in the United States; arrival time at the U.S. port of entry; port of entry arriving at; last country visited; and contact email/phone number for the 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 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 Link: first and last name; date of birth; sex; 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 documents or manually entered their biographic information (if necessary) into CBP Link, they will be prompted to submit the manifest to U.S. Customs and Border Protection. The photograph on the travel document will be collected during the Machine-Readable Zone scan. However, the image is deleted upon submission to U.S. Customs and Border Protection and is not viewed or used by U.S. Customs and Border Protection officers.

Once the data is submitted through CBP Link, U.S. Customs and Border Protection conducts law enforcement checks using U.S. Customs and Border Protection TECS and creates a U.S. Customs and Border Protection Advance Passenger Information System manifest.[21] U.S. Customs and Border Protection officers will then review the manifest and conduct enhanced checks as needed. In addition, U.S. Customs and Border Protection officers use the information submitted through CBP Link to conduct targeting queries and review passengers in advance of

[20] U.S. Customs and Border Protection issues both the carrier code and sender identification to bus carriers. Both codes are unique identifiers and are used to identify the bus carrier company in the Advance Passenger Information System.

[21] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ADVANCE PASSENGER INFORMATION SYSTEM (APIS), DHS/CBP/PIA-001 (2005 and subsequent updates), *available at* Privacy Documents for CBP | Homeland Security.

their arrival at the land border. Once a passenger arrives at the port of entry, officers will process the passenger and match them to the data submitted to the U.S. Customs and Border Protection Advance Passenger Information System through CBP Link.

The carrier code and sender identification collected from the bus driver and submitted through the bus operator persona are sent to the U.S. Customs and Border Protection Advance Passenger Information System and will be written into the U.S. Customs and Border Protection Advance Passenger Information System manifest. This happens at the time of submission. Additionally, at the time of submission, the carrier code and sender identification are immediately erased from CBP Link. All trip and biographic data collected from the bus driver and passengers through the user's mobile device will be deleted from local storage after submission to U.S. Customs and Border Protection, or after 24 hours from collection if the information was never submitted to U.S. Customs and Border Protection.

All data, except for the mobile device information, is submitted through CBP Link and will be forwarded immediately to the Advance Passenger Information System and will not be retained. Advance Passenger Information System data is used for entry screening purposes and is retained for 13 months.[22] While the Advance Passenger Information System only retains information for a limited period, all or a portion of Advance Passenger Information System data is immediately transmitted to the U.S. Customs and Border Protection Automated Targeting System, TECS, and the Arrival and Departure Information System[23] upon receipt. Advance Passenger Information System information is ingested into the following U.S. Customs and Border Protection 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 U.S. Customs and Border Protection Amazon Web Services Cloud Service database.

Air Operator Persona

Landing Rights

To efficiently process arriving international passengers, U.S. Customs and Border Protection must accurately forecast and anticipate the arrival of all international flights. Pursuant to 19 CFR § 122.14, aircraft are required to request permission to land at an airport. U.S. Customs and Border Protection Port Directors or their designated staff are the primary U.S. Customs and

[22] National Archives and Records Administration (NARA) General Records Schedule 5.2 "Transitionary and Intermediary Records" Item 20 covers the destruction of U.S. Customs and Border Protection Advance Passenger Information System records after 13 months.

[23] *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 (2007 and subsequent updates), *available at* Privacy Documents for CBP | Homeland Security.

Border Protection operational points of contact for landing rights, accept landing rights requests, conduct research/analysis, present recommendations, and maintain flight schedules for their respective airports. Air carriers must meet Department of Transportation, Federal Aviation Administration, and Transportation Security Administration requirements for the operation of commercial aircraft in the United States before requesting landing rights from U.S. Customs and Border Protection. To facilitate lawful trade and travel by automating and modernizing current international aircraft arrival and departure processes, U.S. Customs and Border Protection developed a means for commercial air carriers to submit landing rights requests electronically to U.S. Customs and Border Protection to reduce paperwork and facilitate the movement of commercial aircraft into and out of the United States.

To access this functionality in the CBP Link application, air operators must select the "air operator" option from the landing page. Once selected, the air operator will select whether they are a "commercial aircraft-passenger", "commercial aircraft-cargo," or "private aircraft." The operator will then select "Apply for Landing Rights." The operator is first prompted to create a profile for the company, station manager, and ground handler, as necessary. To create a profile, the operator adds their company name, first and last name, email, phone number, and fax number. This can be saved to the account for future use.

The operator can then select "Request Landing Rights," and is prompted to input the airline name, port name, airline code, and bond number. The operator then enters the flight scheduling information (e.g., single or multiple flights, scheduled or unscheduled flight, whether it is a precleared flight, flight number, departure airport, arrival airport, estimated time of arrival/departure, passenger number, terminal, equipment, and any additional comments).

Once complete, the operator is prompted to submit the landing rights application to U.S. Customs and Border Protection. This module in CBP Link will automate and modernize the processes for commercial aircraft entering the United States under provisions of 19 C.F.R. Part 122, Air Commerce Regulations, Subpart B. It is expected that this automation will replace the current methods, allowing for current methods in emergency situations. Once the air operator submits information via CBP Link, the information is sent to backend U.S. Customs and Border Protection systems and stored for 365 days.

Fair Information Practice Principles

The U.S. Department of Homeland Security conducts Privacy Impact Assessments on developed or procured information technology systems involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form, as required by Public Law

107-347, Section 208, "The E-Government Act of 2002," and any applicable and implementing Office of Management and Budget guidance; or proposed rulemakings affecting personal information as required by Section 222(a)(4) of the Homeland Security Act of 2002; or technologies that sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information pursuant to 6 U.S.C § 142(a)(1).

In response to these obligations, the U.S. Department of Homeland Security Privacy Office developed a set of Fair Information Practice Principles[24] from the underlying concepts of the Privacy Act of 1974[25] to encompass the full scope of the information and interactions of the U.S. Department of Homeland Security. The Fair Information Practice Principles account for the nature and purpose of the information being collected in relation to the U.S. Department of Homeland Security's mission to preserve, protect, and secure. The Fair Information Practice Principles are a set of eight principles that are rooted in the tenets of the Privacy Act.

3. What specific legal authorities and/or agreements permit the collection of information by the project in question?
The legal authority that permits the collection of information by CBP Link varies depending on the purpose for which the information is being collected. Various authorities authorize U.S. Customs and Border Protection to collect data regarding all travelers entering and departing the United States. *See, e.g.*, The Immigration and Nationality Act 211, 215, 231 (8 U.S.C. 1181, 1185, 1221), and Tariff Act of 1930, as amended, 71 Public Law 361, sec 433, 46 Stat. 590, 711 (19 U.S.C. 1433). Also s*ee* 8 CFR 215.8, 8 CFR 235.1. U.S. Customs and Border Protection has authority to conduct inspections of persons, vessels, aircraft, vehicles, and merchandise involved in importation under 5 U.S.C. 301; 19 U.S.C. 66, 1592, 1593a, 1624, 6 U.S.C. 101, 8 U.S.C. 1324(b). Under 19 U.S.C. 1431(b), U.S. Customs and Border Protection has the authority to collect manifest data from vessels, aircraft, or vehicles entering the United States. In addition to the mandatory submissions provided by both commercial air and vessel carriers and private aircraft pilots, U.S. Customs and Border Protection receives voluntary Advance Passenger Information System submissions from rail and bus carriers. Pursuant to 19 CFR § 122.14, aircrafts are required to request permission to land at an airport. 49 U.S.C. § 114(f)(8), (9) authorizes the Transportation Security Administration the authority

[24] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum 2008-01, 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.
[25] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

to use biometric and other technologies to prevent persons who may pose a danger to air safety or security from boarding an aircraft.

4. Will this information be maintained as part of system of records,[26] as defined in the Privacy Act, 5 U.S.C. §552a?

The following System of Records Notices provide coverage for CBP Link:

- DHS/CBP-001 Import Information System;[27]
- DHS/CBP-005 Advance Passenger Information System;[28]
- DHS/CBP-006 Automated Targeting System;[29]
- DHS/CBP-021 Arrival and Departure Information System;[30] and
- DHS/ALL-002 Department of Homeland Security Mailing and Other Lists System.[31]

5. From which population does the project collect, maintain, use, and/or disseminate personally identifiable information[32]?

☒ a. Members of the public

☒ b. U.S. Department of Homeland Security employees and/or contractors

☐ c. Other federal employees

[26] The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
[27] *See* DHS/CBP-001 Import Information System, 81 Fed. Reg. 48826 (July 26, 2016), *available at* System of Records Notices (SORNs) | Homeland Security.
[28] *See* DHS/CBP-005 Advance Passenger Information System, 80 Fed. Reg. 13407 (March 13, 2015), *available at* System of Records Notices (SORNs) | Homeland Security.
[29] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* System of Records Notices (SORNs) | Homeland Security.
[30] *See* DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 Fed. Reg. 72081 (November 18, 2015), *available at* System of Records Notices (SORNs) | Homeland Security.
[31] *See* DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (November 25, 2008), *available at* System of Records Notices (SORNs) | Homeland Security.
[32] Personally identifiable information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. *See* OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information.

6. What personally identifiable information is collected, maintained, used, or disseminated?

Regardless of the functionality, CBP Link users are required to create a user profile. To create a user profile, the CBP Link 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 or biometric information is collected or stored locally on the mobile device or in web storage.

The information users provide through CBP Link depends on the function of CBP Link that the individual is using. For example, brokers/carriers/forwarders must submit business information, such as company name and importer identification, in addition to the point of contact's own biographic information, such as name and email address, to schedule inspections. Information provided by or about members of the public includes additional biographic and biometric information (e.g., first and last name; date of birth; sex; country of citizenship; country of residence; travel document information, and photograph) that U.S. Customs and Border Protection will use to verify identity and use for screening and vetting, if applicable. For certain functionalities, CBP Link may also capture geolocation[33] information from users' devices (i.e., to determine whether an individual is in a defined proximity outside of the United States). If geolocation is needed, CBP Link prompts the user to enable location services on their phone.[34] Different functions may also require users to submit a "selfie."

U.S. Customs and Border Protection may also publish function-specific Privacy Impact Assessments that fully discuss the information users submit to CBP Link to accomplish the various functions within CBP Link.

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

[34] While CBP Link is a voluntary application, certain functionalities within the application require the use of location services to ensure users are in a defined proximity. Location services must be enabled to ensure any information is submitted to U.S. Customs and Border Protection.

7. What is the intended use of personally identifiable information?
CBP Link allows users to interact with the U.S. Department of Homeland Security for a variety of purposes. The information collected via CBP Link is used for a variety of U.S. Department of Homeland Security mission-related purposes and in any standalone function-specific Privacy Impact Assessment. As described above, certain CBP Link functionality uses geolocation information, for example, to determine whether an individual is in a defined proximity to the United States border or outside of the United States. Certain CBP Link functionalities may also use photographs submitted by users to validate identity and confirm that the person is "live," employing liveness detection capabilities. U.S. Customs and Border Protection may share information collected through CBP Link both internally and externally to the U.S. Department of Homeland Security, consistent with applicable law and policy. However, no sharing will come directly from CBP Link. Any information sharing, pursuant to applicable system of records notices and the associated information sharing arrangements completed from the backend system of record in which the data resides.

8. How long and under which retention schedule is the information retained?
CBP Link collects and stores the first and last name of the user upon profile creation. This information is stored locally on the mobile device or within browser storage to create a user profile within CBP Link so that the user can quickly retrieve information for subsequent uses. No other biographic information is stored on the mobile device or within the browser storage. The user profile information is stored locally until the user chooses to delete the application. The retention of information submitted through CBP Link depends on the function the individual is using, and the backend system to which U.S. Customs and Border Protection sends the submitted information. The standalone, function-specific Privacy Impact Assessments will fully discuss the retention of the data collected through CBP Link and any privacy risks related to retention.

9. With whom will personally identifiable information be shared?	
☒ Within the Component/Office	Specify: U.S. Customs and Border Protection
☒ Other U.S. Department of Homeland Security Component(s)/Office(s)	Specify: Transportation Security Administration (Transportation Document Checker functionality)
☐ State, local, tribal, or territorial entities	Specify:

☐ Public	Specify:
☐ Private sector	Specify:
☐ Foreign governments	Specify:
☐ Foreign entities	Specify:
☐ Other:	Specify:

10. How are individuals provided notice prior to the collection of information? If notice is not provided, explain why not.

CBP Link is available for download on Android and iPhone Operating System mobile devices through the Google or Apple mobile application stores, as well as on the Internet via web browser. CBP Link contains Terms and Conditions, including a privacy policy, that appear every time a user logs in. The Terms and Conditions outline the type of information collected, how the information will be used, and how the information will be shared. Users must accept these terms prior to being authorized to use any CBP Link functionality.

As new use cases are developed and implemented, the U.S. Department of Homeland Security may conduct targeted outreach to specific populations for certain CBP Link functionalities or issue media releases to encourage use of the application. U.S. Customs and Border Protection will update this Privacy Impact Assessment as new CBP Link functionalities are added or modified. U.S. Customs and Border Protection may also conduct standalone, function-specific Privacy Impact Assessments for new functions as necessary for additional transparency.

11. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out?

CBP Link is public-facing and voluntarily available for the public to use. Users select which function they want to use and must authenticate their identity prior to using the application. Users are presented with a privacy policy when they access the application to understand why U.S. Customs and Border Protection is collecting information and how it will be used.

12. What procedures are in place to allow individuals to correct inaccurate or erroneous information?

Any member of the public may voluntarily download CBP Link from the mobile application store on his or her mobile device. CBP Link is available for members of the public and/or entities that need to interact with U.S. Customs and Border Protection, so long as the mobile or web application supports the function that the user is trying to complete.

In addition, CBP Link contains Terms and Conditions, to include a privacy policy, that appears every time a user logs in. Users must accept these terms prior to being authorized to use any CBP Link functionality. Depending on the functionality, CBP Link also uses "just-in-time" notifications that require a user's acknowledgment before the application can access camera or location services, for example.

Some functions of CBP Link allow users to submit information on behalf of other people. Specifically, 19 U.S.C. §1431(b), U.S. Customs and Border Protection has the authority to collect manifest data from vessels, aircraft, or vehicles entering the United States. In addition to the mandatory submissions provided by both commercial air and vessel carriers and private aircraft pilots, U.S. Customs and Border Protection receives voluntary Advance Passenger Information System submissions from rail and bus carriers.

A bus operator may also submit bus manifest information to U.S. Customs and Border Protection through CBP Link. In this scenario, an individual may not have the opportunity to consent to the submission or use of their information.

If users submit incorrect information through CBP Link, they can resubmit new information or contact the U.S. Customs and Border Protection Information Center online or by calling 1-877-227-5511 to determine how to update their submission. Individuals may request information about records contained in the source systems that CBP Link 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://www.dhs.gov/foia-contact-information.

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 the U.S. Department of Homeland Security 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, U.S. Customs and Border Protection 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 U.S. Customs and Border Protection does not require a specific form, guidance for filing a request for information is available on the U.S. Department of Homeland Security website at http://www.dhs.gov/file-privacy-act-request.

All or some of the requested information may be exempt from access pursuant to the Privacy Act to prevent harm to law enforcement investigations or other interests as permitted by law.

Finally, when a traveler arrives in the United States, he or she may correct or update any information during the inspection process that was submitted through the CBP Link that is deemed incorrect or inaccurate. For example, if an operator inadvertently submits inaccurate data through CBP Link, this information can be updated during the inspection process.

13. What administrative, technical, and physical controls are used to protect the information?

CBP Link uses two-factor authentication and strong encryption to transfer any data submitted through the application to U.S. Customs and Border Protection backend systems. Additionally, the CBP Link uses Login.gov to manage users' authentication by allowing users to sign in with an email address, password, and multi-factor authentication method (e.g., face or touch unlock on mobile device, text message/email one-time code verification), and conduct identity proofing by verifying an individual's asserted identity. Login.gov ensures a secure connection and identity verification when using the CBP Link mobile application. Individuals with a Login.gov account can sign into multiple government websites (including CBP Link) with the same email address and password. Consistent with Login.gov standard operating procedures, the email address used to create the Login.gov account is sent to U.S. Customs and Border Protection for access and storage.

The information collected through CBP Link is used for various mission-related purposes and resides in various U.S. Customs and Border Protection systems. Therefore, the security controls of those systems protect the information. Additionally, U.S. Customs and Border Protection has analyzed the application to ensure that information is sent only to U.S. Customs and Border Protection, and the application can only access the information necessary to complete the functions.

14. How does the Component ensure that personally identifiable information is used

appropriately?
All information collected through CBP Link is sent to backend systems of record for various U.S. Department of Homeland Security-mission related purposes. U.S. Customs and Border Protection implements role-based access for all U.S. Customs and Border Protection systems and only grants access to users who have a demonstrated need to know. All U.S. Customs and Border Protection systems secure its data by complying with the requirements of U.S. Department of Homeland Security information technology security policy, particularly the U.S. Department of Homeland Security Sensitive Systems Policy Directive 4300A.[35] This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. U.S. Customs and Border Protection periodically evaluates these systems to ensure that it complies with these security requirements. Each system provides audit trail capabilities to monitor, log, and analyze system transactions as well as actions and system accesses of authorized users. U.S. Customs and Border Protection periodically conducts reviews for compliance within the program and between external partners to ensure that the information is used in accordance with the stated acceptable uses documented in the Memoranda of Understanding/Agreement, System of Record Notice, sharing agreements, and other technical and business documentation.

Associated Privacy Risks and Mitigations

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**. The CBP Link uses Login.gov to manage users' authentication by allowing users to sign in with an email address, password, and multi-factor authentication method, and conduct identity proofing by verifying an individual's asserted identity. Login.gov ensures a secure connection and identity verification when using CBP Link. Certain functionalities within CBP Link require an individual to provide information to confirm the person submitting the information matches the information submitted by the individual. For example, a "selfie" is collected to confirm the individual's identity. U.S. Customs and Border Protection uses the Traveler Verification Service as the backend matching service to conduct a facial comparison matching between the "selfie" and the

[35] *See* DHS 4300A Sensitive Systems Handbook, *available at* https://www.dhs.gov/publication/dhs4300a-sensitive-systems-handbook.

	photograph in U.S. Customs and Border Protection holdings. For functionalities that require the submission of a photograph, a photograph must be submitted for each individual (i.e., each family member) the submission is regarding. CBP Link is embedded with software that performs a "liveness" test to determine that it is a real person (and not a picture of a person). Once authenticated, there are functionalities of CBP Link that require information to be submitted on behalf of, and without consent of the individual the information is pertaining to. For example, an operator may submit manifest information to U.S. Customs and Border Protection in anticipation of the traveler's arrival to the United States. This submission allows U.S. Customs and Border Protection to conduct critical pre-arrival vetting to yield information on outstanding wants or warrants, and information from other government agencies regarding high-risk parties; enables U.S. Customs and Border Protection to confirm the accuracy of that information by comparison with information obtained from the traveler and from the carriers; and facilitates making immediate determinations as to a traveler's security risk. Although consent is not required, the operator or carrier may provide notice to the traveler that theirs will be shared with U.S. Customs and Border Protection.

Privacy Risk:	There is a risk that geolocation information (i.e., latitude, longitude) collected from users using certain CBP Link functions may be used inconsistently with applicable law and policy.
Mitigation:	This risk is **fully mitigated.** Geolocation information collected from CBP Link users is used to confirm the location of an individual as required based on the functionality they are attempting to use within the application. If the application function requires a user to be outside of the United States, the geolocation information can confirm that the user is outside of the United States.

Privacy Risk:	There is a risk that users will submit inaccurate information about other people.
Mitigation:	This risk is **fully mitigated.** Although U.S. Customs and Border Protection cannot prevent users from submitting inaccurate information on behalf of themselves or other people, U.S. Customs and Border Protection can verify the information before retaining it as accurate. It is unlikely that a user will submit inaccurate information on about another person because there is no

	benefit in submitting inaccurate information through CBP Link. In some cases, the submission of the inaccurate information could subject the user to monetary or legal penalties. In addition, any specific privacy risks related to data quality and integrity will be addressed in any standalone, function-specific Privacy Impact Assessments.

Contact Official

Jody Hardin
Executive Director, Innovation and Strategy
Office of Field Operations
U.S. Customs and Border Protection
U.S. Department of Homeland Security

Responsible Official

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

Approval Notice:

By signing below, the U.S. Department of Homeland Security Chief Privacy Officer approves this Privacy Impact Assessment for CBP Link. If, however, during the operational course of this program or U.S. Customs and Border Protection's use of this technology changes from what has been documented or the U.S. Department of Homeland Security Privacy Office becomes aware of evidentiary changes to the intended use of the personally identifiable information or the scope of the personally identifiable information collected, of the program or technology is determined to be ineffective, the Chief Privacy Officer reserves the right to revoke approval of this Privacy Impact Assessment.

Approval Signature

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

_____

Roman Jankowski
Chief Privacy Officer
U.S. Department of Homeland Security
Privacy@hq.dhs.gov