Privacy Impact Assessment

for the

CBP Home

DHS Reference No. DHS/CBP/PIA-084

June 25, 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 Customs and Border Protection (CBP) launched a public-facing mobile application, CBP Home, in support of the Presidential Proclamation *Establishing Project Homecoming*. Project Homecoming offers an incentivized, voluntary program for aliens in the United States illegally to leave the country. U.S. Customs and Border Protection is conducting this Privacy Impact Assessment to address privacy risks in the collection, maintenance, use, and dissemination of the information collected by CBP Home, which may include the collection of U.S. citizen and Lawful Permanent Resident information.

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.
On May 9, 2025, President Donald J. Trump issued the Presidential Proclamation that established Project Homecoming.[2] The U.S. Department of Homeland Security is designing Project Homecoming to facilitate voluntary self-departures for aliens illegally present in the United States. As part of Project Homecoming, illegal aliens can use the CBP Home mobile application's "Submit Intent to Depart" function to notify the U.S. Department of Homeland Security of their intent to depart the country. Under Project Homecoming, aliens may be eligible for financial incentives, such as travel assistance (departure flight funded by the government) and a $1,000 stipend upon verification of departure from the United States. Aliens who have departed the United States can use CBP Home's "Voluntary Self-Reported Exit" function to verify their departure.

[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* https://www.whitehouse.gov/presidential-actions/2025/05/establishing-project-homecoming/.

The use of CBP Home is intended for aliens illegally present in the United States to report their intent to depart or verify their departure. However, submissions may include information about U.S. citizen or Lawful Permanent Resident co-travelers, typically children or other dependents.

Submit Intent to Depart

Illegal aliens and their co-travelers (users) can use CBP Home to submit their intention to depart from the United States for review, vetting, and processing by the U.S. Department of Homeland Security. Upon opening the app, a pop-up notification within CBP Home will ask the user to enable location services on their phone for geolocation purposes.[3] The user is prompted to select their preferred language, and the next screen then displays that the U.S. Government will cover travel costs and a $1,000 exit bonus.

The user is then prompted to enter biographic information, such as his or her full name, date of birth, country of citizenship, email address, and phone number. CBP Home then prompts the traveler to take a "selfie." The mobile application instructs the alien to line up their face with a box and to perform a "liveness" test to determine that it is a real person (and not a picture of a person).[4] Once the "selfie" is captured, the user is asked to review his or her personal information, and may edit the information, as necessary. Once reviewed, the user can add additional individuals to their group by repeating the same steps. Once complete, CBP Home displays a message notifying the user that someone will reach out to follow up on their submission.

Upon submission, U.S. Customs and Border Protection matches the biographic information and photograph against U.S. Customs and Border Protection holdings. If the photo and biographic data match, the biographic information, photograph, and location information are transferred to a segregated database within the U.S. Customs and Border Protection Automated Targeting System.[5] The data is then transmitted to the U.S. Immigration and Customs Enforcement's Enforcement Integrated Database[6] for further enforcement checks and to make a final

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

[4] While the applicant is taking the "selfie," the technology embedded within the mobile application relies on the device's 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 applicant is unable to proceed with submitting their exit through the CBP Home mobile application.

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM, DHS/CBP/PIA-006 (2007 and subsequent updates), *available at* Privacy Documents for CBP | Homeland Security.

[6] The Enforcement Integrated Database is a U.S. Department of Homeland Security-shared common database repository used by several DHS law enforcement and homeland security applications. The Enforcement Integrated Database stores and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by the U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, and U.S. Customs and

determination on eligibility. In the interest of public safety and the integrity of the United States immigration system, and to preserve the U.S. economy, it is vital that the U.S. Immigration and Customs Enforcement collect this intended departure information so that resources are not inadvertently expended seeking to remove aliens who have already or will soon depart the United States. Providing means for compliant aliens to voluntarily report their intended departure allows government resources to focus efforts on apprehending illegal aliens who do not intend to depart.

Upon submission, the user will receive an automated email confirming the submission of their intent to depart through CBP Home. If no additional information is needed, the email will notify the user that they will be contacted by the U.S. Department of Homeland Security to facilitate next steps, including collecting additional information to facilitate the departure from the United States. In some circumstances, the user will be notified of their requirement to register with the U.S. Citizenship and Immigration Services as part of the Alien Registration Requirement, to be eligible for participation in Project Homecoming.[7]

Voluntary Self-Reported Exit

Once an alien has departed the United States, the alien can use CBP Home to self-report his or her exit from the United States. Similar to the Submit Intent to Depart functionality, the CBP Home app requires location services to be turned on. CBP Home will perform a one-time geolocation ping to ensure the mobile device user is outside of the United States. If the mobile device's geolocation is confirmed to be outside the United States, the user is permitted to continue to the next step in the process.

CBP Home prompts the user that he or she must meet the following requirements to successfully record their exit: (1) must have a passport or valid Alien Registration Number, (2) must be at least 3 miles outside of the United States, and (3) must have good lighting to capture a quality and usable "selfie". On the next screen, the user selects which identification they will be entering into the app (e.g., passport or Alien Registration Number) as well as the associated identification details (document/identification number, country of citizenship/issuance) to select the type of identification. The next screen asks the user to input their name, date of birth, sex, and email address, and select the country in which they are currently present while reporting their exit.

The next step is for the traveler to take a "selfie," and perform the liveness test, as described for the intent to depart function. Once successfully captured, the traveler can review the submission

Border Protection. The Enforcement Integrated Database supports Immigration and Customs Enforcements' processing and removal of noncitizens from the United States. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE, DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* Privacy Documents for ICE | Homeland Security.

[7] *See* https://www.uscis.gov/alienregistration.

details before submission to the U.S. Customs and Border Protection. After reviewing the information, the traveler selects "submit." The traveler can then complete the same steps for their co-travelers.

Upon submission, the U.S. Customs and Border Protection uses the biographic and travel document information submitted by the traveler 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 U.S. Customs and Border Protection 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 traveler voluntarily reporting their exit.[8] If there is a match to the "selfie," then the traveler's exit is recorded as a biometrically confirmed exit in U.S. Customs and Border Protection TECS (not an acronym),[9] the Arrival and Departure Information System,[10] and the U.S. Office of Biometric Identity Management Automated Biometric Identification System/Homeland Advanced Recognition Technology.[11] If the Traveler Verification Service is not able to successfully match the source photograph from Customs and Border Protection holdings to the "selfie," the mobile device user will receive a message to "Try Again Later, or 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.

[8] *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* DHS/CBP/PIA-056 Traveler Verification Service | Homeland Security.

[9] *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.

[10] *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.

[11] CBP enrolls alien travelers in the U.S. Office of Biometric Identity Management Automated Biometric Identification System 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, DHS/OBIM/PIA-001 (2012), *available at* DHS/OBIM/PIA-001 Automated Biometric Identification System | Homeland Security. The U.S. Department of Homeland Security is replacing the Automated Biometric Identification System with the Homeland Advanced Recognition Technology System 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, *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* DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System Increment 1 | Homeland Security.

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

Fair Information Practice Principles (FIPPs)

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[12] from the underlying concepts of the Privacy Act of 1974[13] 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?

Section 1(c) of the Presidential Action *Establishing Project Homecoming* states, "in furtherance of the purposes of this proclamation, and to facilitate the rapid departure of illegal aliens from the United States, I [Donald J. Trump] direct, pursuant to section 215(a)(1) of the INA (8 U.S.C. 1185(a)(1)), the Secretary of State and the Secretary of Homeland Security to take all appropriate actions to enable the rapid departure of illegal aliens from the United States who currently lack a valid travel document from their countries of citizenship or nationality or who desire to travel to any other country willing to accept their entry."

Additionally, the U.S. Department of Homeland Security has broad authority to require aliens

[12] 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.
[13] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

to provide biometrics and other relevant identifying information upon entry to, or exit from, the United States under various provisions of the Immigration and Nationality Act of 1952, as amended. Specifically, the U.S. Department of Homeland Security may control alien entry and exit and inspect aliens under sections 215(a) and 235 of the Immigration and Nationality Act (8 U.S.C. §§ 1185, 1225). As part of its entry and exit controls, the U.S. Department of Homeland Security may require aliens to provide fingerprints, photographs, or other biometrics upon arrival in, or exit from, the United States, and select classes of aliens may be required to provide information at any time pursuant to the Immigration and Nationality Act 214, 215(a), 235, 262(a), 263(a), 264(c), (8 U.S.C. §§ 1184, 1185(a), 1225, 1302(a), 1303(a), 1304(c)); 8 U.S.C. § 1365b. The federal statutes requiring the U.S. Department of Homeland Security to create a biometric entry and exit system to record the arrival and exit of aliens include, but are not limited to: Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208, 110 Stat. 3009-546; Section 2(a) of the Immigration and Naturalization Service Data Management Improvement Act of 2000, Public Law 106-215, 114 Stat. 337; Section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106-396, 114 Stat. 1637, 1641; Section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56, 115 Stat. 272, 353; Section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. No. 107-173, 116 Stat. 543, 552; Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, 118 Stat. 3638, 3817; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-52, 121 Stat. 266; and Section 802 of the Trade Facilitation and Trade Enforcement Act of 2015, Public Law 114-125, 130 Stat. 122, 199 (6 U.S.C. § 211(c)(10)).

4. Will this information be maintained as part of system of records,[14] as defined in the Privacy Act, 5 U.S.C. §552a?

To the extent any records are covered by the Privacy Act, the following System of Records Notices provide coverage for CBP Home:

- DHS/CBP-006 Automated Targeting System,[15] which covers the collection and maintenance of information collected via CBP Home.

[14] 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.

[15] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* System of Records Notices (SORNs) | Homeland Security.

- DHS/CBP-021 Arrival and Departure Information System,[16] which serves as the record of travelers' departure (and arrivals) into and out of the United States.

5. From which population does the project collect, maintain, use, and/or disseminate personally identifiable information[17]?

☒ a. Members of the public

☐ b. DHS employees and/or DHS contractors

☐ c. Other federal employees

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

As described above, the use of CBP Home is intended for aliens illegally present in the United States to report their intent to depart or verify their departure. However, submissions may include information about U.S. citizen or Lawful Permanent Resident co-travelers, typically children or other dependents.

Aliens choosing to use CBP Home are asked to provide biographic information, including but not limited to, full name, date of birth, country of citizenship, email address, phone number, sex, Alien Registration Number, and travel document (e.g., passport) information. CBP Home also requires aliens to submit a "selfie" of themselves and will perform a "liveness" test to determine that the submission is from a real person and not a picture of a person.

CBP Home also captures geolocation[18] information from users' devices to confirm the alien's location and/or to determine whether the alien is outside of the United States when self-

[16] *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.

[17] 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

[18] 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.

reporting his or her exit. CBP Home prompts the user to enable location services on their phone to collect the geolocation.[19]

7. What is the intended use of the personally identifiable information?

The information collected via CBP Home is used for a variety of U.S. Department of Homeland Security mission-related purposes, including identity verification, vetting, facilitating travel assistance, and to self-report a departure from the United States. The U.S. Department of Homeland Security uses the geolocation information to determine the location of the alien and/or to confirm he or she is outside of the United States when self-reporting his or her exit. The U.S. Customs and Border Protection uses the photographs submitted by users to validate identity and to ensure that the information submission is coming from a real person.

The information collected via CBP Home will be shared both internally and externally, consistent with applicable law and policy.

CBP Home serves as the means for an alien to self-deport. However, the information is automatically shared upon submission with the U.S. Immigration and Customs Enforcement's Enforcement Integrated Database. The Immigration and Customs Enforcement uses the information to complete enforcement checks and screening, facilitate travel assistance, and deprioritize enforcement and removal activities. To facilitate travel assistance, the U.S. Immigration and Customs Enforcement will share select information with an external organization that will contact aliens to facilitate their departure outside of the United States.

U.S. Customs and Border Protection shares information with U.S. Immigration and Customs Enforcement from the Automated Targeting System, consistent with applicable law.

8. How long and under which retention schedule is the information retained?

[19] While CBP Home 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.

Information collected as part of the Submit Intent to Depart functionality is sent to and stored in the Automated Targeting System. The Automated Targeting System retains information for 15 years. As described above, upon submission, information is immediately ingested into the U.S. Immigration and Customs Enforcement's Enforcement Integrated Database and stored for 75 years.

Information collected as part of the Voluntary Self-Reported Exit functionality is sent to the CBP Amazon Cloud Service and stored for one year. Biographic information (name, travel document information, and date of submission) is then sent to the Arrival and Departure Information System via TECS. The Arrival and Departure Information System is the system of record for all U.S. arrivals and departures and is stored for 75 years.

9. With whom will the 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: U.S. Immigration and Customs Enforcement
☐ 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.

Project Homecoming launched a nationwide communications campaign to inform illegal aliens of the program and of the consequences of remaining, including removal, prosecution, fines, wage garnishment, and property confiscation.

The communications campaign includes, but is not limited to the White House's issuance of several media releases encouraging the use of CBP Home to self-deport. Furthermore, President Donald J. Trump issued a Presidential Action, *Establishing Project Homecoming* with a

corresponding Fact Sheet[20] on May 9, 2025. Additionally, the U.S. Department of Homeland Security has issued several media releases describing CBP Home and the use of the application by an alien to submit their intent to depart and to self-report his or her exit. Finally, this Privacy Impact Assessment serves as an additional form of notice.

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

CBP Home is public-facing and voluntarily available for the public to use. Within the respective app store, users are presented with Terms and Conditions which include the privacy policy outlining the purpose of the collection, and how it is used and shared. CBP Home also uses "just-in-time" notifications that require a user's acknowledgment before the application can access camera or location services.

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

Any member of the public may voluntarily download CBP Home from the mobile application store on his or her mobile device. CBP Home allows users to submit information on behalf of other people. For example, a parent could submit their intent to depart or self-report an exit on behalf of his or her minor child. If aliens submit incorrect information through CBP Home for the Submit Intent to Depart functionality, the alien can correct information before submission, or when contacted as a follow-up to their submission. When self-reporting an exit, if the alien suspects that they may have submitted inaccurate information, they can submit a redress request through the DHS Traveler Redress Inquiry Program at TRIP@tsa.dhs.gov.[21]

Additionally, aliens may 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 Home populates through procedures provided by the Freedom of Information Act (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

[20] *See* https://www.whitehouse.gov/fact-sheets/2025/05/fact-sheet-president-donald-j-trump-establishes-project-homecoming/.
[21] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRAVELER REDRESS INQUIRY PROGRAM, DHS/ALL/PIA-002 (2007 and subsequent updates), *available at* Privacy Documents for Department-Wide Programs | Homeland Security.

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, the 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.

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

CBP Home uses two-factor authentication and strong encryption to transfer any data submitted through the application to U.S. Customs and Border Protection backend systems. 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 Home 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 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.[22] 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 they comply with these security requirements. Each system provides audit trail capabilities to monitor, log, and analyze system transactions as well as actions and system accesses of authorized users. 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 CBP Home collects more information than necessary.
Mitigation:	This risk is **fully mitigated**. The CBP Home mobile application collects limited information in order to accomplish the intended functions of the app. Any additional necessary information is collected through a separate process, outside of the mobile application. CBP Home is intended to be a user-friendly experience.

Privacy Risk:	There is risk that geolocation information (i.e., latitude, longitude) collected from users using certain CBP Home functions may be used in ways that are not consistent with applicable law and policy.
Mitigation:	This risk is **partially mitigated**. Geolocation information collected from CBP Home users is used to confirm the location of an individual. The Voluntary Self-Reported Exit function requires a user to be outside of the United States. CBP Home performs a one-time geolocation ping to ensure

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

	the mobile device user is outside of the United States. Therefore, the geolocation information is used only to confirm that the submission is outside of the United States.

Privacy Risk:	There is risk that users will submit inaccurate information about other people or submit information on behalf of another individual without their consent.
Mitigation:	This risk is **partially 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 verifies the information submission against information within CBP holdings. It is unlikely that a user will submit inaccurate information about another person because there is no benefit in submitting inaccurate information through CBP Home.

Privacy Risk:	There is a risk that users will not receive notice on the collection, maintenance, use, and dissemination of their information.
Mitigation:	This risk is **fully** mitigated. As described above, Project Homecoming launched a nationwide communications campaign to inform illegal aliens of the program and of the consequences of remaining, including removal, prosecution, fines, wage garnishment, and property confiscation. The communications campaign includes, but is not limited to the White House's issuance of several media releases encouraging the use of CBP Home to self-deport. Furthermore, President Donald J. Trump issued a Presidential Action, *Establishing Project Homecoming* with a corresponding Fact Sheet[23] on May 9, 2025. Additionally, the U.S. Department of Homeland Security has issued several media releases describing CBP Home and the use of the application by an alien to submit their intent to depart and to self-report his or her exit. CBP also issued notice and a list of Frequently Asked Questions on the CBP website.[24] Finally, this Privacy Impact Assessment serves as an additional form of notice.

[23] *See* https://www.whitehouse.gov/fact-sheets/2025/05/fact-sheet-president-donald-j-trump-establishes-project-homecoming/.
[24] *See* https://www.dhs.gov/cbphome.

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 Home. 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

Original, signed copy on file with the U.S. Department of Homeland Security Privacy Office.

_____

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