



# Privacy Impact Assessment Update

for the

## Electronic System for Travel Authorization (ESTA)

DHS Reference No. DHS/CBP/PIA-007(i)

April 26, 2024



Homeland  
Security



## Abstract

The Electronic System for Travel Authorization (ESTA) is an application and screening system used to determine whether citizens and nationals from countries participating in the Visa Waiver Program (VWP)<sup>1</sup> are eligible to travel to the United States. The U.S. Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is publishing this Privacy Impact Assessment (PIA) update for ESTA to provide notice and assess the privacy risks associated with recent enhancements to ESTA, including (1) sharing national identifier numbers received from ESTA applicants with the country that issued the identification number, to obtain information about the ESTA applicant as part of the International Biometric Information Sharing (IBIS) Program; and (2) updates to the ESTA mobile application.

## Overview

As previously described in the ESTA Privacy Impact Assessment series, the Visa Waiver Program is a rigorous security partnership that promotes secure travel to the United States while also facilitating U.S. passport-holders' travel to Visa Waiver Program partner nations. Since its inception in 1986, the Visa Waiver Program has evolved into a comprehensive security partnership with many of the United States' closest allies. DHS uses a risk-based, multi-layered approach to detect and prevent terrorists, criminals, and other mala fide actors from traveling to the United States. This approach incorporates regular, national-level risk assessments concerning the impact on U.S. national security, immigration, and law enforcement interests of each program country's participation in the Visa Waiver Program. It also includes a comprehensive application process through the ESTA website or mobile application, as well as vetting of travelers prior to their departure for the United States, upon arrival at U.S. ports of entry, and during subsequent encounters within the United States.<sup>2</sup>

Eligibility for a country's designation in the Visa Waiver Program is defined in Section 217 of the Immigration and Nationality Act (INA) (including as amended most recently by the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015).<sup>3</sup> Among other

---

<sup>1</sup> The Visa Waiver Program, administered by DHS in consultation with the Department of State, permits citizens of designated participating countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those designated participating countries must permit U.S. citizens and nationals to travel to their countries for a similar length of time without a visa for business or tourism purposes.

<sup>2</sup> CBP's ESTA is an application and screening system used to determine whether citizens and nationals from countries participating in the Visa Waiver Program are eligible to travel to the United States. A Visa Waiver Program traveler who intends to arrive at a U.S. port of entry must obtain an approved ESTA travel authorization to be considered for admission to the United States. The application collects biographic information, a photograph, and responses to questions related to an applicant's eligibility to travel under the Visa Waiver Program.

<sup>3</sup> See generally 8 U.S.C. § 1187 (providing that the Secretary of Homeland Security, in consultation with the Secretary of State, may designate certain countries as Visa Waiver Program countries if specified requirements are



requirements, the Passenger Information Exchange provision of the statute specifies that any country seeking to participate in the Visa Waiver Program enter “into an agreement with the United States to share information regarding whether citizens and nationals of that country traveling to the United States represent a threat to the security or welfare of the United States or its citizens, and fully implement such agreement.”<sup>4</sup>

CBP is publishing this Privacy Impact Assessment update for ESTA to provide notice and assess the privacy risks associated with recent enhancements to ESTA, including (1) sharing national identifier numbers received from ESTA applicants with the country that issued the identification number, to obtain information about the ESTA applicant as part of the IBIS Program, and (2) updates to the ESTA mobile application.

### **International Biometric Information Sharing Program (IBIS)**

DHS, in consultation with the Department of State, assessed that establishing direct biometric information sharing partnerships under the IBIS Program<sup>5</sup> would meet the intent of the eligibility requirements for designation in the Visa Waiver Program as enumerated in 8 U.S.C. § 1187(c)(2)(F), Section 217 of the Immigration and Nationality Act.<sup>6</sup> As a result, DHS and State announced the new Enhanced Border Security Partnership (EBSP) biometric information sharing requirement, which all Visa Waiver Program countries will need to complete for initial and continued designation in the Visa Waiver Program. DHS is continuing to implement IBIS relationships with Visa Waiver Program countries over the next five years.

IBIS enables automatic comparison of the fingerprints collected by DHS or a foreign partner on travelers, border crossers, suspected criminals, asylum seekers, irregular migrants, refugees, and other individuals encountered by government representatives against U.S. and

---

met, including: (1) a U.S. Government determination that the country meets the applicable statutory requirement with respect to nonimmigrant visitor visa refusals for nationals of the country; (2) a U.S. Government determination that the country extends or agrees to extend reciprocal privileges to citizens and nationals of the United States; (3) an official certification that it issues machine-readable, electronic passports that comply with internationally accepted standards; (4) a U.S. Government determination that the country’s designation would not negatively affect U.S. law enforcement and security interests; (5) an agreement with the United States to report, or make available through other designated means, to the U.S. Government information about the theft or loss of passports; (6) a U.S. Government determination that the government accepts for repatriation any citizen, former citizen, or national not later than three weeks after the issuance of a final executable order of removal; and (7) an agreement with the United States to share information regarding whether citizens or nationals of the country represent a threat to the security or welfare of the United States or its citizens.

<sup>4</sup> 8 U.S.C. § 1187 (c)(2)(F). The requirement to implement the agreement was added by the Visa Waiver Improvement and Terrorist Travel Prevention Act of 2015 (Pub. L. No. 114-113), enacted on December 18, 2015.

<sup>5</sup> The DHS International Biometric Information Sharing Program (IBIS) principally facilitates fingerprint-based bilateral biometric and biographic information sharing between the United States and a foreign partner. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INTERNATIONAL BIOMETRIC INFORMATION SHARING PROGRAM (IBIS), DHS/ALL/PIA-095 (2022 and subsequent updates), *available at* <https://www.dhs.gov/privacy-documents-department-wide-programs>.

<sup>6</sup> 8 U.S.C. § 1103, et. seq. The Visa Waiver Program provisions have been codified at 8 U.S.C. § 1187.



partner country terrorism, national security, identity, immigration, and criminal records. IBIS helps the United States to identify individuals who present a threat to the security or welfare of the United States, identify perpetrators of identity fraud in the immigration process, enhance the vetting of individual travelers, and verify eligibility for an immigration or humanitarian benefit. It similarly allows foreign partners to compare fingerprints against DHS records for the same purposes. Every IBIS partnership begins with cooperation under a negotiated bilateral agreement or arrangement instrument. The relevant agreement or arrangement provides a flexible but enduring framework to facilitate information exchange for criminal, border and national security, immigration, and counterterrorism purposes at high volumes, requiring minimal manual intervention for each disclosure. These bilateral instruments outline specific expectations for appropriate handling and protection of personal data exchanged.

### **ESTA Mobile Application**

In 2023, CBP launched a new mobile application in which applicants and representatives may submit ESTA applications using a smartphone or tablet.<sup>7</sup> The ESTA application on the mobile application collects the same biographic information as the ESTA application on the website. In addition, the mobile application retrieves the information from an applicant's passport eChip and captures a "selfie" of the applicant. CBP collects the passport photograph through the eChip and the applicant's "selfie" photograph to complete a 1:1 biometric identity verification using those two images and conduct vetting. When the ESTA application is submitted to CBP, the vetting process begins and the mobile application will display a status that the ESTA application is pending until vetting is complete. When the vetting process is complete, the mobile application will display whether an ESTA authorization is approved, not authorized, or pending, as described above. All ESTA applications submitted via the ESTA mobile application are stored in the ESTA system along with ESTA applications received via the website. The 2023 ESTA Privacy Impact Assessment update noted that no information is stored locally on the user's device or in the ESTA mobile application itself.

## **Reason for the PIA Update**

CBP is publishing this Privacy Impact Assessment update for ESTA to provide notice and assess the privacy risks associated with recent enhancements to ESTA, including (1) sharing national identifier numbers received from ESTA applicants with the country that issued the identification number, to obtain information about the ESTA applicant as part of the IBIS program, and (2) updates to the ESTA mobile application.

---

<sup>7</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION (ESTA), DHS/CBP/PIA-095(h) (2023), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



## **IBIS**

In February 2022, DHS introduced a requirement that each Visa Waiver Program country establish an Enhanced Border Security Partnership through the IBIS Program with DHS. Under the Enhanced Border Security Partnership, the Visa Waiver Program country would allow DHS to routinely screen against the biometric records of the Visa Waiver Program country's biometrics holdings. These holdings include biometrics of travelers to the United States who have a nexus to the Visa Waiver Program country, including its citizens and nationals; applicants for immigration benefits or humanitarian protection in the United States; and individuals encountered by DHS in a border screening or immigration context in the United States.

While the ESTA application does not enable the collection of fingerprints, some Visa Waiver Program countries issue unique national identifier numbers which are associated with the individual's biometrics upon issuance. DHS assesses these biometrically-anchored national identifier numbers serve the same function as a biometric in enabling accurate identification of individuals and identity resolution. CBP already collects these national identifying numbers from ESTA applicants.

Under its Enhanced Border Security Partnerships arrangement, a foreign partner may authorize DHS and DHS components to conduct a search against their relevant national databases using the national identification number when an individual provides their national identification number to CBP on the ESTA application. CBP will pull the national identification number from the individual's ESTA application and initiate an automated search to the foreign partner's holdings using that national identification number. In the event of a match of the applicant's national identification number, consistent with the terms of the bilateral information sharing arrangement between DHS and the foreign partner, the foreign partner will provide information to CBP on the associated biographic identity (name, date of birth, travel documents, nationality), any known criminal convictions and arrests for serious crimes, and an indication of the individual's immigration status in the partner country.<sup>8</sup>

The identity information the foreign partner provides back to CBP in the event a national identification number-based match occurs will be stored in the Automated Targeting System (ATS)<sup>9</sup> and handled in the same manner as other vetting results yielded during the vetting process. Within the Automated Targeting System, the information received from the foreign partner will be marked as originating from a foreign partner, enabling CBP to appropriately safeguard the information and ensure onward use and sharing of the data is consistent with the relevant bilateral agreement and applicable DHS policies. This enhancement does not require any other changes to

---

<sup>8</sup> "Serious crimes" include all crimes considered felonies under U.S. law.

<sup>9</sup> See U.S. DEPARTMENT OF HOMELAND SECURITY, U.S CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM (ATS), DHS/CBP/PIA-006 (2007 and subsequent updates), available at <https://www.dhs.gov/privacy-documents-us-customs-and-border-protection>.



existing ESTA processes or systems, and there are no changes to the collection, use, retention, or sharing of personally identifiable information (PII) under ESTA or IBIS.

## **The ESTA-IBIS Process**

When CBP receives an ESTA application from a national or citizen of a country included in Appendix B of the November 2, 2022, IBIS Privacy Impact Assessment, CBP will retrieve the national identification number from the ESTA application using the Automated Targeting System and submit the identification number to the respective foreign partner to determine if the foreign partner has a matching identity record.<sup>10</sup> The foreign partner will indicate to CBP in the Automated Targeting System whether there is a “match” or “no match” to the national identification number in their respective system. When there is no match or if the receiving country’s national law or bilateral agreement prohibits the disclosure of the match, the foreign partner will return a “no match” response and no further information will be exchanged. When there is a match based on the national identification number, the home countries may exchange the type of information as defined by the relevant bilateral agreement or arrangements included in Appendix A to the November 2, 2022, IBIS Privacy Impact Assessment according to their respective laws and policies to assist in border security or immigration benefit adjudication decisions. CBP then creates a record within the Automated Targeting System to store the matching results from the foreign country.

## **ESTA Mobile Application**

As described in the June 2023 ESTA Privacy Impact Assessment update, CBP launched the ESTA mobile application as another means for applicants to submit their ESTA application to CBP. Applicants may voluntarily choose to use the ESTA mobile application instead of the application on the ESTA website. With this Privacy Impact Assessment update, CBP is launching the optional ability for users to retrieve their ESTA application, submitted through the website or mobile application, by enabling biometric authentication on their phone and creating a profile for easy access to their ESTA application and travel authorization.<sup>11</sup>

## **Biometric Authentication**

Many mobile devices enable users to choose to enroll their biometrics (e.g., face,

---

<sup>10</sup> Routine Use G of DHS/CBP-009 ESTA System of Records Notice permits CBP to share information to an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where CBP believes the information would assist enforcement of applicable civil or criminal laws and such disclosure is proper and consistent with the official duties of the person making the disclosure. *See* DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 87 Fed. Reg. 41338 (July 12, 2022), *available at* <https://www.dhs.gov/system-records-notices-sorns>.

<sup>11</sup> Biometric authentication is an alternative to traditional passwords or personal identification numbers in identity authentication and is the process of uniquely identifying an individual using biometrics (e.g., fingerprints or facial features) when accessing features on the ESTA mobile application.



fingerprint) to unlock and access features on their mobile device using their own biometrics instead of inputting additional credentials (e.g., passcode, username/password). Once biometrics are enrolled on the phone, the user can look at or touch their device to unlock, access, and/or approve additional features.

The ESTA mobile application will now offer users the option to use their stored biometrics on their own mobile device to access their ESTA application instead of entering a username and password each time. This enhancement benefits the user by enabling alternative access to their ESTA application. CBP will **not** be able to access any information that is stored on a user's device. This new, optional, voluntary feature enables the ESTA mobile application to verify a user's identity and securely access or input their information within the mobile application.<sup>12</sup> All biometrics are stored locally on a user's mobile device (not in the application), consistent with the terms and conditions of the user's mobile device platform. CBP does not have access to, nor does it store, the biometrics used for logging in to the mobile application.

For a first-time user, after downloading the mobile application and reviewing the Privacy Act Statement and accepting the security notification, a pop-up will be presented to the user to enable them to store their ESTA application information and make it retrievable using their biometrics (stored on their mobile device) when subsequently accessing the mobile application. Previous ESTA mobile application users will be presented with the option to enable biometric authentication once and will either choose "Enable Biometric Authentication" or "No Thanks." [See Figure 1 below] If a user chooses to store their information and enable biometric authentication, the app will navigate to the "Home" screen. When the user searches for an application or creates a new application, they will be prompted to allow the system to use biometrics to access and store the ESTA application on the mobile application. [See Figures 2 and 3 below] If a user has an existing application, the user can select "Find It" to view an existing ESTA application. If users are biometrically authenticated, they are shown their list of stored applications. From here, they can click on an existing application, or search for an application using their passport information and application number. In the latter case, their application will be saved to their stored applications list (on the mobile application) upon successful retrieval.

For new applications, users will complete the application process normally until their application number is generated by clicking the "NEXT" button on the "Applicant Information" page. If the user is not authenticated but is enrolled in biometrics, the mobile application will authenticate them and will store their ESTA application upon successful authentication.<sup>13</sup> If the

---

<sup>12</sup> This biometric authentication aligns with the National Institute of Standards and Technology's 800-63-3 IAL2 guidelines, available at <https://pages.nist.gov/800-63-3/sp800-63-3.html>.

<sup>13</sup> An applicant is asked to authenticate when they either click the 'NEXT' button on the Applicant Information page when creating a new application or select 'Find It' to view an application. If, during a session, the applicant has not searched for an application prior to creating a new application, this scenario would occur.

user is already authenticated, their ESTA application will be automatically stored within the mobile application on their mobile device.

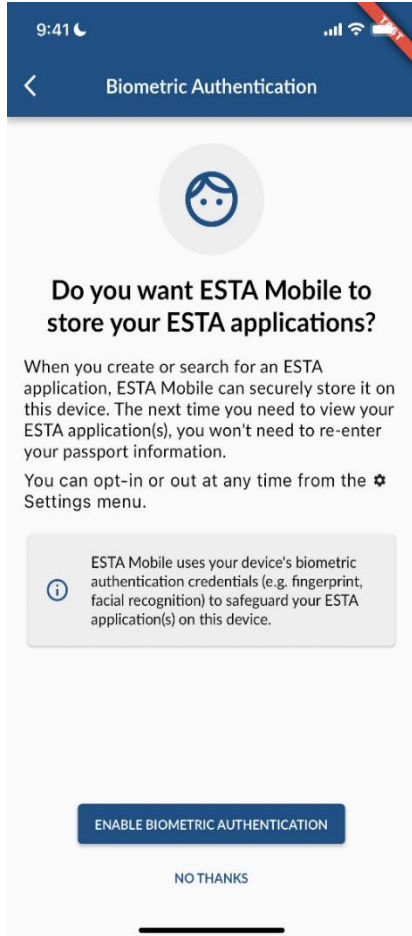


Figure 1. Consent to enable biometric authentication functionality.

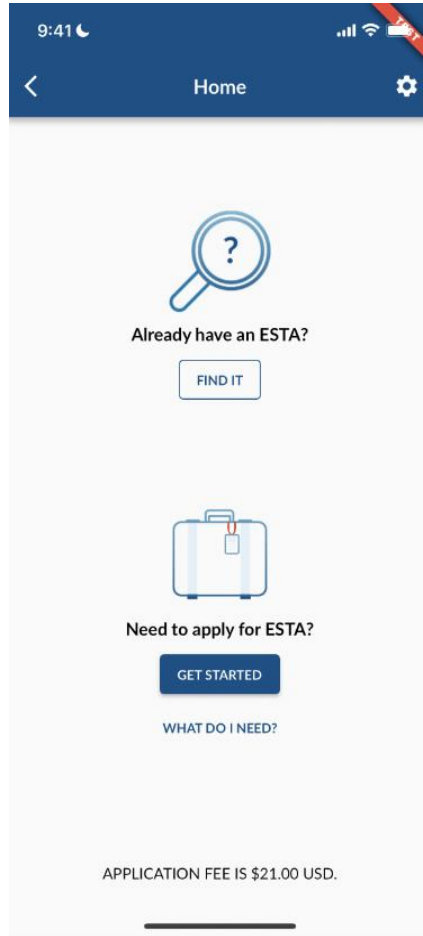


Figure 2. View for a new or returning ESTA applicant.

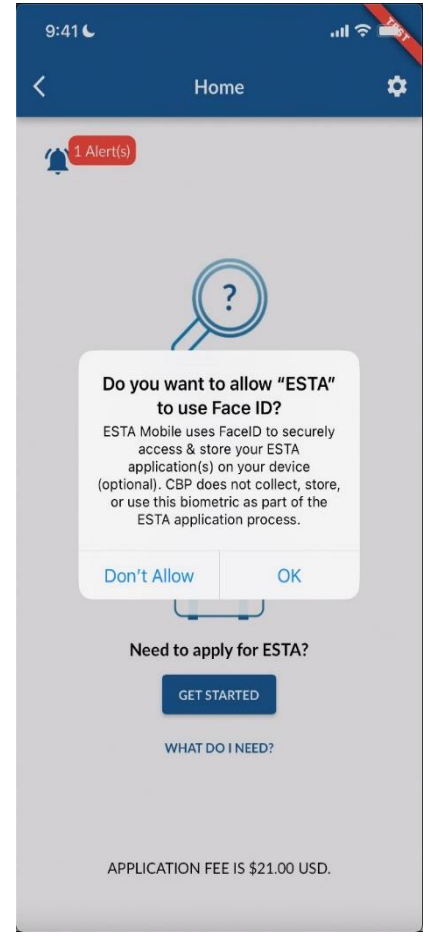


Figure 3. Consent to enable the mobile application to use Face ID.

## Privacy Impact Analysis

### Authorities and Other Requirements

#### IBIS

Eligibility for a country’s designation in the Visa Waiver Program is defined in Section 217 of the Immigration and Nationality Act. Among other requirements, the “Passenger Information Exchange” section of the statute specifies that any country seeking to participate in the Visa Waiver Program enter “into an agreement with the United States to share information regarding whether citizens and nationals of that country traveling to the United States represent a





threat to the security or welfare of the United States or its citizens, and fully implement such agreement.”<sup>14</sup>

The purpose of DHS’s Visa Waiver Program information sharing policy and the IBIS Program is to allow DHS to compare information of travelers and immigration benefit applicants, as well as those encountered during border inspections or in criminal investigations, against foreign partners’ appropriate identity records in addition to criminal and terrorist records. Information gleaned from this sharing is used to prevent, detect, and investigate crime, including assessing whether an individual presents a criminal or terrorist risk, and aids border and immigration-related decisions.

Routine Use G of the ESTA System of Records Notice (SORN) permits CBP to share information with an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where CBP assesses the information would assist enforcement of applicable civil or criminal laws and such disclosure is proper and consistent with the official duties of the person making the disclosure. The DHS/CBP-006 Automated Targeting System System of Records Notice<sup>15</sup> accounts for the storage of vetting results, including those obtained from the respective partner country.

### **ESTA Mobile App**

There are no changes to CBP authorities and other requirements to operate ESTA with this Privacy Impact Assessment update.

### **Characterization of the Information**

#### **IBIS**

With this update, under IBIS sharing, CBP may use information received on an ESTA application pursuant to the IBIS program and may receive additional information from a foreign partner that issued a traveler’s national identifier number. In the event of a match, consistent with the terms of the bilateral information sharing arrangement, the foreign partner will provide information to CBP regarding the associated identity, any known criminal convictions and arrests for serious crimes, and an indication of the individual’s immigration status. Consistent with other ESTA vetting results, these results will be stored in the Automated Targeting System separate from the ESTA application.

**Privacy Risk:** There is a risk that personal information originally collected by CBP to grant travel authorization will be shared with foreign partners who use that information for

---

<sup>14</sup> See supra note 6.

<sup>15</sup> See DHS/CBP-006 Automated Targeting System (ATS), 77 Fed. Reg. 30297 (May 22, 2012), available at <https://www.dhs.gov/system-records-notices-sorns>.



unauthorized purposes, which may be incompatible with the original purpose of the CBP collection.

**Mitigation:** This risk is mitigated. CBP will only disclose pursuant to an IBIS agreement the national identification number the applicant knowingly provides to CBP when submitting an ESTA application. The country receiving that data should already have that data because it would have issued the national identification number. If there is a match, the country only becomes aware that the individual has applied for an ESTA. The foreign partner commits to only use that information consistent with the bilateral information sharing agreement or arrangement to assist in border security or immigration benefit adjudication decisions. If the national identification number does not match an existing record in the partner's system, the knowledge of that identification number does not reveal anything about the individual, except that an individual provided to CBP an incorrect or false national identification number.

### **ESTA Mobile App**

There are no changes to the collection of information with this Privacy Impact Assessment update. ESTA mobile application users may opt into storing information on their mobile device to support biometric authentication. With this implementation, CBP is not collecting or retaining any new or additional information. CBP does not have access to, nor does it store, the biometrics used for logging in to the mobile application.

### **Uses of the Information**

#### **IBIS**

This update does not impact the use of information. CBP continues to use the information yielded as part of the ESTA vetting process to grant or deny a travel authorization. With this update, CBP will share the national identification number received through ESTA applications with the foreign partner pursuant to an IBIS agreement. In the event of a national identification number match, the foreign partner may, consistent with its applicable laws, provide CBP with information to 1) assist in verifying an individual's identity for immigration purposes and assessing whether an individual presents a criminal or terrorist risk; 2) aid CBP in border screening; and 3) aid in making admissibility and immigration-related decisions.

#### **ESTA Mobile App**

This update does not impact the use of information. CBP does not use or have access to biometric information stored on the individual's mobile device. The biometric authentication information is solely used to enable the user to access their ESTA information within the ESTA mobile application. There are no other uses of this information.



## Notice

### **IBIS**

CBP is providing notice of these changes through the publication of this Privacy Impact Assessment. Additionally, DHS is concurrently issuing a Privacy Impact Assessment update to IBIS Privacy Impact Assessment to document these changes.

**Privacy Risk:** There is a risk that ESTA applicants are not aware that CBP is sharing their information with the foreign partner that issued their national identifier number.

**Mitigation:** This risk is partially mitigated. When accessing the ESTA application, users are presented with a Security Notification, Disclaimer, and Privacy Act Statement. These notices outline the purpose of the collection and use of the information, including conducting law enforcement checks and sharing with external partners. Users are required to review and acknowledge these notices before proceeding with the ESTA application. By acknowledging these notices, the user consents to the uses of information outlined the notice. Furthermore, DHS is providing additional transparency through the publication of this Privacy Impact Assessment and an update to the IBIS Privacy Impact Assessment.

### **ESTA Mobile App**

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

## **Data Retention by the Project**

### **IBIS**

There are no new risks to data retention. CBP continues to store ESTA vetting results in the Automated Targeting System (ATS) in accordance with the Automated Targeting System retention period, consistent with what was stated in the previous ESTA Privacy Impact Assessment series.

### **ESTA Mobile App**

The June 2023 ESTA Privacy Impact Assessment update noted that the mobile application does not retain any data, even on a temporary basis. With this Privacy Impact Assessment update, users may now choose to store information on their mobile device. CBP does not collect or retain any additional biometric information as part of the biometric authentication process. Users may choose to delete their stored ESTA application from their mobile device at any time.

**Privacy Risk:** There is a risk that CBP will retain the biometric information that is used to enroll the user in biometric authentication.



**Mitigation:** This risk is mitigated. CBP does not retain any biometric authentication information as part of the biometric authentication process. This information is solely used to enable the user to access their information within the ESTA mobile application. There is no other retention of this information.

## **Information Sharing**

### **IBIS**

CBP will continue to share ESTA application information, which may include the national identification number, with other federal government authorities, including Intelligence Community partners. CBP may share ESTA information on a case-by-case basis to appropriate state, local, tribal, territorial, or international government agencies as described in the previous ESTA Privacy Impact Assessment series. In addition, the national identification number from the ESTA application will now be shared with the foreign partner who issued the applicant's national identifier number.

In the event of a national identification number match, the foreign partner may, consistent with its applicable laws, provide CBP with information to 1) assist CBP in verifying an individual's identity for immigration purposes and assessing whether an individual presents a criminal or terrorist risk; 2) aid CBP and foreign partners in border screening; and 3) aid in making border and immigration related decisions. These purposes are documented in the relevant international agreement or arrangement negotiated with the IBIS partner country. DHS limitations on use of personal information in information-sharing relationships are documented in applicable agreements, arrangements, and other implementing documentation. For example, these agreements and arrangements define the purpose of the collection and scope for which the information can be used, limit onward sharing, and require partners to ensure the data is secured and safeguarded.

### **ESTA Mobile App**

There are no changes to information sharing because of the implementation of the biometric authentication. CBP does not have access to, nor does it store the biometrics used for logging in to the mobile application.

## **Redress**

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

## **Auditing and Accountability**

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



## Contact Official

Ray Provencio  
(A) Executive Director  
Admissibility and Passenger Programs  
Office of Field Operations  
U.S. Customs and Border Protection

## Responsible Official

Debra L. Danisek  
CBP Privacy Officer  
Privacy and Diversity Office  
U.S. Customs and Border Protection  
[privacy.cbp@cbp.dhs.gov](mailto:privacy.cbp@cbp.dhs.gov)

## Approval Signature

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

---

Mason C. Clutter  
Chief Privacy Officer  
U.S. Department of Homeland Security  
(202) 343-1717