Privacy Impact Assessment Update

for the

Electronic System for Travel Authorization (ESTA)

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

June 7, 2023

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)[1] 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 the launch of a new mobile application. The ESTA program and information collection has undergone several enhancements since the previous Privacy Impact Assessment published on September 1, 2016.[2]

Overview

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. ESTA information is necessary to issue a travel authorization consistent with the requirements of Form I-94W.[3] 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. Visa Waiver Program travelers (hereinafter referred to as applicants, or their representatives)[4] submit ESTA applications to CBP to include name, country of birth and citizenship, date of birth, sex, travel document information, contact information (e.g., phone and email address), social media handle and platform (optional), parents' names, employment

[1] 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.

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ELECTRONIC SYSTEM FOR TRAVEL AUTHORIZATION, DHS/CBP/PIA-007 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[3] The ESTA program allows CBP to eliminate the requirement that Visa Waiver Program travelers complete Form I-94W prior to being admitted to the United States because the ESTA application electronically captures duplicate biographical and travel data elements collected on the paper Form I-94W. *See* https://www.cbp.gov/document/forms/form-i-94w-visa-waiver-arrivaldeparture-record.

[4] To accommodate people who may not have familiarity with or access to computers or the internet, DHS designed ESTA to allow a third party, such as a relative, friend, or travel agent, to submit an application on behalf of the traveler. In all cases, the traveler is responsible for the answers submitted on the traveler's behalf by a third party and the third party must check the box on the ESTA application indicating that the third party completed the application on the traveler's behalf. The email address provided should be the traveler's email address. If the traveler does not have an email address, an alternative third-party email address belonging to a point of contact (*e.g.*, a family member, friend, or business associate) must be provided.

information, destination address, U.S. point of contact information, as well as responses to questions related to an applicant's eligibility to travel under the Visa Waiver Program.

CBP uses the biographic information submitted as part of the ESTA application to conduct vetting against selected security and law enforcement databases at DHS, including TECS[5] and the Visa Waiver Program (ATS),[6] as well as publicly available sources (e.g., social media websites, even if the applicant opts out of providing social media information), as described in previously published Privacy Impact Assessments in the ESTA series.

ESTA applicants or representatives can check the status of their application online via the ESTA website. The website will display one of the following statuses:

Authorization Approved – The travel authorization has been approved and the applicant is authorized to travel to the United States under the Visa Waiver Program. A travel authorization does not guarantee admission to the United States as a CBP officer at a port of entry will make the final determination regarding admissibility.

Travel Not Authorized – The applicant is not authorized to travel to the United States under the Visa Waiver Program. The applicant may be able to obtain a visa from the Department of State for travel. Please visit the Department of State website at http://www.travel.state.gov for additional information about applying for a visa. This response does not deny entry into the United States. This response only prohibits the applicant from traveling to the United States under the Visa Waiver Program.

Authorization Pending – The applicant's travel authorization is under review because an immediate determination could not be made on the application. This response does not indicate negative findings.

If travel is not authorized for the ESTA applicant, the applicant is not eligible to travel to the United States under the Visa Waiver Program.[7] If the application is approved, the approval establishes that the traveler is eligible to travel to the United States under the Visa Waiver Program but does not guarantee that the traveler is admissible to the United States. Upon arrival to a United States port of entry, the Visa Waiver Program traveler will be subject to an inspection by a CBP officer who may determine that the traveler is inadmissible for any reason under United States law. ESTA

[5] *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 TECS SYSTEM PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection

[6] *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(e) (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[7] Applicants denied a travel authorization to the United States via ESTA may still apply for a nonimmigrant visa from the Department of State at a U.S. Embassy or Consulate.

travel authorizations are valid for two years from the date of authorization, or until the Visa Waiver Program traveler's passport expires, whichever comes first.[8] An ESTA authorization generally permits the traveler to travel to the United States for multiple trips over a period of two years eliminating the need for a traveler to reapply during the validity period.

Reason for the PIA Update

With this Privacy Impact Assessment update, CBP is documenting several enhancements and changes to the ESTA program to include: (1) expanded collection to include a picture of an applicant's biographic passport page (for ESTA website submission only), (2) a new ESTA mobile application, (3) newly approved National Archives and Records Administration (NARA) ESTA retention schedule; (4) clarification regarding countries designated as state sponsors of terrorism; and, (5)discussion of the requirement to obtain an ESTA authorization for land travel.

1. ESTA Website Optical Character Recognition of Passport Biographic Data Page

As described above, the ESTA application requires several key pieces of biographic information, which can be found on the passport biographic data page (e.g., name, date and place of birth, country of citizenship). Additionally, this page contains a photograph of the passport holder. Historically, applicants and representatives manually input this information by typing their biographic information from the passport into the ESTA website. To alleviate the need to manually input information, CBP now requires applicants and representatives to "capture" or "upload" a picture of the applicant's passport page, depending on the method of submission.[9] The use of the "capture" or "upload" feature relies on an optical character recognition (OCR) scan to auto-populate the information from the passport into the ESTA application on the website. CBP requires this new mandatory upload of the passport biographic page to (a) mitigate the potential for applicants or representatives to inadvertently enter inaccurate information into the website such as typos or inverted birth dates and (b) allow the system to identify potential ineligible documents and flag the applications for manual review prior to authorization.

To begin, an applicant or representative selects the "Upload Your Passport" on the ESTA website. To "capture" a picture of the passport's biographic data page, the applicant or representative must use a device with a camera, such as an Android or an iOS device (e.g., browser on a phone or tablet). The device prompts the applicant or representative to take a picture of the passport's biographic data page using the device's camera. Applicants and representatives can also "upload" a picture of the biographic passport data page if a camera is not detected on the device

[8] For more general ESTA information, *see* http://www.cbp.gov/travel/international-visitors/esta.
[9] Applicants and representatives can "upload" a scanned copy or previously taken photograph from the user's photo album from a desktop computer. Alternatively, if the user is submitting the *website* application through a mobile device or tablet (but not through the mobile application), the mobile website browser is enabled to allow users to "capture" or in other words, take a live photograph of the biographic passport page.

(e.g., desktop computer), or the applicant or representative does not physically possess the passport.

When uploading a picture, the applicant or representative selects a pre-scanned image in .gif, .png, .jpg, and .jpeg file format to upload onto the ESTA website. Once the picture of the biographic passport data page is "captured" or "uploaded," a preview of the image will appear in a new window for the applicant or representative to verify that the image is clear and not too blurry or dark. Additionally, the window will display the biographic information from the passport (e.g., full name, date and place of birth, passport number) that was auto-populated into the window from the passport scan. In the rare instance that the biographic information was not properly converted by the optical character recognition scan, applicants and their representatives may edit the information to ensure accuracy.

After the image of the biographic passport page is either "captured" or "uploaded," the applicant or representative is prompted to input the remaining biographic information into the application including: phone number and email address; information about current or previous employer; social media information (optional); destination address and point of contact in the United States; and emergency point of contact information. Consistent with the existing process, the applicant or representative is also required to answer Visa Waiver Program eligibility questions regarding communicable diseases, arrests and convictions for certain crimes, history of visa revocation or deportation, as well as other questions. Once the applicant or representative supplies the requested information, they are directed to make a payment. Payment is made using the U.S. Department of Treasury's Pay.gov service.[10] Once Pay.gov validates the payment information, the ESTA website displays that payment was successfully submitted. The applicant or representative is then prompted to submit the application to CBP.

Once an application is submitted, CBP will automatically vet the ESTA biographic information against security and law enforcement databases at DHS. The image of the biographic passport page is stored in the ESTA database for identity reconciliation purposes. Once CBP completes the vetting process, the ESTA website notifies the applicant whether their authorization is approved, travel not authorized, or travel pending, as described above.

2. New Mobile Application for ESTA submissions

In 2023, CBP launched a new mobile application in which applicants and representatives may submit ESTA applications using a smartphone or tablet. The ESTA mobile application is available for download on both Android and iOS mobile devices. Once the applicant or representative downloads the mobile application to a mobile device, they are presented with the

[10] Pay.gov collects payment information—either credit card, debit card, or Automated Clearing House (ACH) debit from a personal bank account. *See* U.S. Department of Treasury Financial Management Services Pay.Gov Privacy Impact Assessment 2.0 (July 1, 2011), *available at* https://fiscal.treasury.gov/files/pia/paygov-pia.pdf.

"Welcome" screen. On this screen, the applicant or representative selects the preferred language to complete the application and reads and acknowledges the Security Notification[11] and the ESTA Privacy Act Statement. Once these steps are completed, the applicant or representative selects "Get Started" to proceed with completing the application. The applicant or representative is first asked to indicate their role (e.g., applicant or a third-party representative). To use the mobile application, the applicant or representative must be in possession of the traveler's passport.

To begin the ESTA application submission, the applicant or their representative is prompted to "capture" the Machine-Readable Zone (MRZ) of the passport. The ESTA mobile application will display a pop-up notifying the applicant or representative that the mobile application is accessing the mobile device's camera. Once the camera is enabled, the mobile application prompts the applicant or representative to position the mobile device's camera over the passport's Machine-Readable Zone.

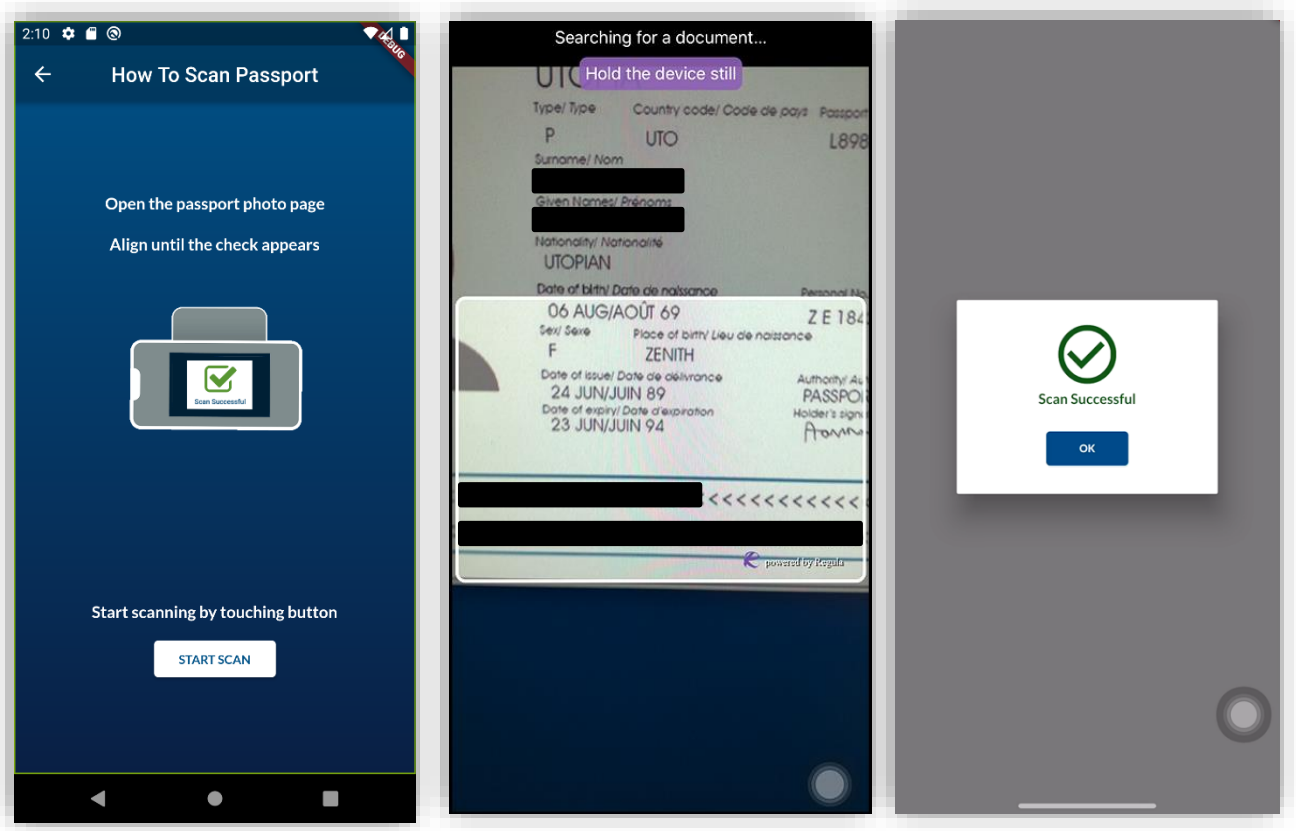

Figure 1: ESTA Mobile App MRZ Scan

[11] The Security Notification notifies the user that the user is about to access a DHS system. The Disclaimer notifies the user that the information provided in the mobile application is used to perform checks against law enforcement databases. It also says that a determination that the applicant is not eligible for ESTA authorization does not preclude them from applying for a visa to travel to the United States.

The device then scans the Machine-Readable Zone to capture and retrieve biographic information from the passport including name, passport number, nationality, date of birth, sex, and passport expiration date. This biographic information is then automatically populated into the ESTA application of the mobile application to eliminate the need for the applicant or representative to manually input certain information.

After the biographic information is populated into the mobile application, the applicant or representative is prompted to place their mobile device near the passport's electronic chip (eChip), a Radio Frequency Identification (RFID)-enabled chip that contains the same information that is printed on the passport's data page: the holder's name, date of birth, and other biographic information as well as a biometric identifier.[12] By placing the mobile device near the eChip, the mobile device enables the Near Field Communication (NFC)[13] capability to wirelessly retrieve the

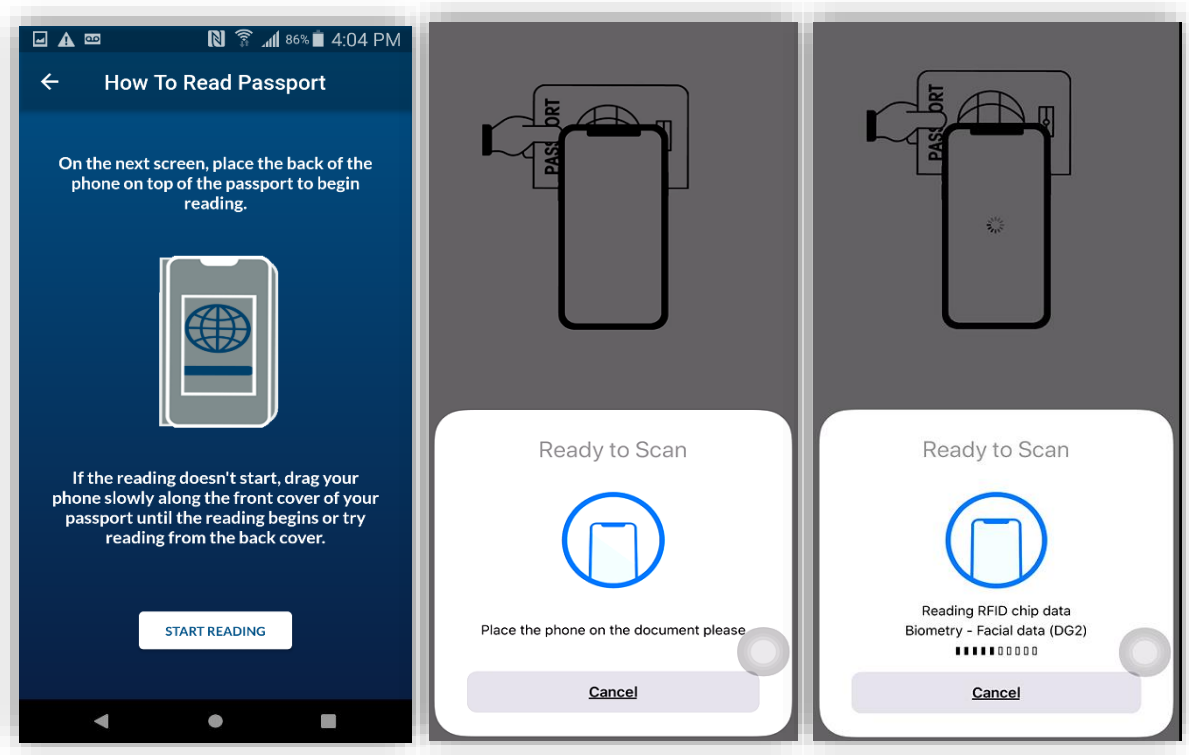

Figure 2: ESTA Mobile App Passport NFC retrieval of passport biometrics

[12] The United States requires that the chip contain a digital photograph of the holder. All e-Passports issued by designated countries participating in the Visa Waiver Program and the United States have security features to prevent the unauthorized reading or "skimming" of data stored on the e-Passport chip.

[13] Near Field Communication describes a technology which can be used for contactless exchange of data over short distances. Two Near Field Communication-capable devices are connected via a point-to-point contact over a short distance. This connection can be used to exchange data between the devices.

biometric data stored within the eChip. The only biometric information on the eChip is the passport photograph and country signing certificate to certify the authenticity of the passport.

Once the mobile application retrieves the photograph from the eChip, the mobile application prompts applicants to take a live photograph or "selfie" of the applicant (representatives will be taken to the next screen). The mobile application instructs the ESTA applicant to line their face up with a box and to perform a "liveness" test to determine that it is a real person (and not a picture of a person).[14] Once complete, the mobile application takes the photograph. CBP uses the "selfie" image to conduct one-to-one (1:1) facial comparison against the passport photograph previously uploaded to the ESTA mobile application from the eChip. Using the Traveler Verification Service (TVS), CBP compares the two photographs to conduct a 1:1 match with the "selfie" and passport photograph to biometrically verify the applicant's identity.[15] If the two photographs are a match, the Traveler Verification Service will send a match response back to ESTA. In the rare event that the Traveler Verification Service is unable to match

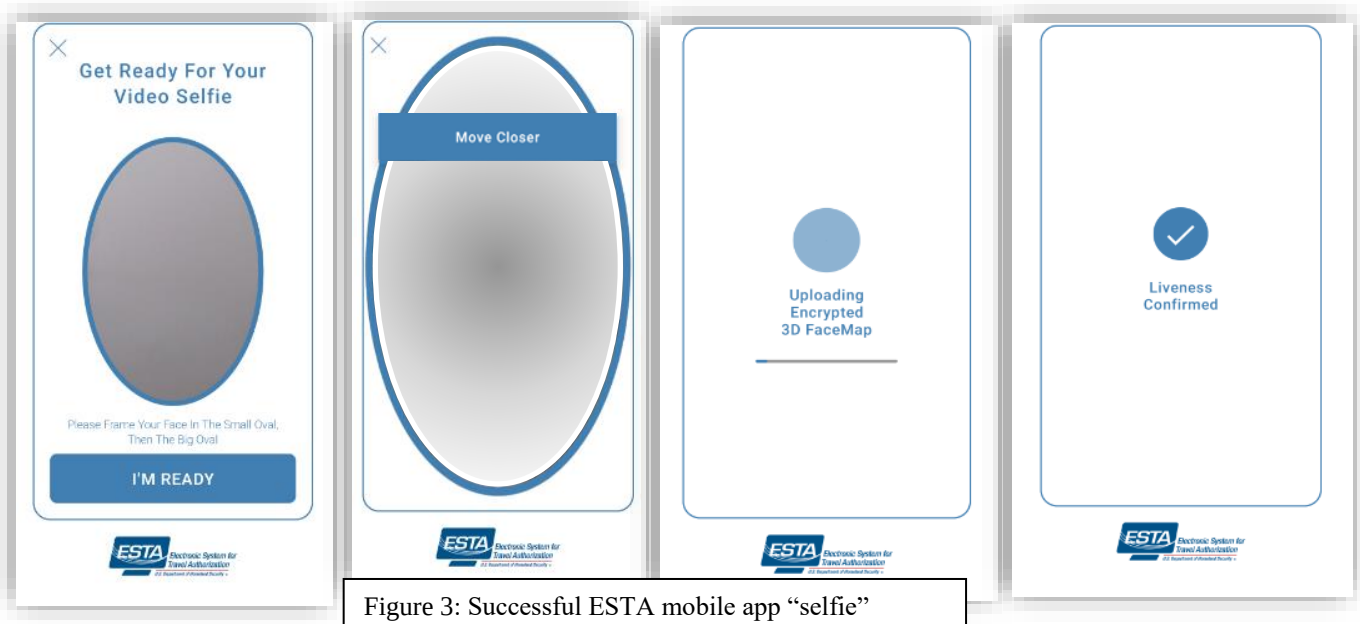

Figure 3: Successful ESTA mobile app "selfie"

[14] While the applicant is taking the "selfie," the technology embedded within the mobile application relies on the devices camera to view a live image through 3D face changes and observing perspective distortion to prove the image is 3D. If "liveness" cannot be confirmed, the applicant is unable to proceed with submitting the application through the ESTA mobile application.

[15] CBP's Traveler Verification Service is an accredited information technology system consisting of a group of similar systems and subsystems that support the core functioning and transmission of data between CBP applications and partner interfaces. Since early 2017, CBP has used the Traveler Verification Service as its backend matching service for all biometric entry and exit operations that use facial recognition, regardless of air, land, or sea. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TRAVELER VERIFICATION SERVICE, DHS/CBP/PIA-056 (2018), *available at* https://www.dhs.gov/privacydocuments-us-customs-and-border-protection.

the "selfie" to the passport photograph, the mobile application will prompt the applicant to retake a "selfie." An applicant can attempt to retake the selfie up to three times. If after three attempts the Traveler Verification Service cannot match the two photographs, the mobile application will default to a third-party submission to allow for the submission of the application without the "selfie."[16]

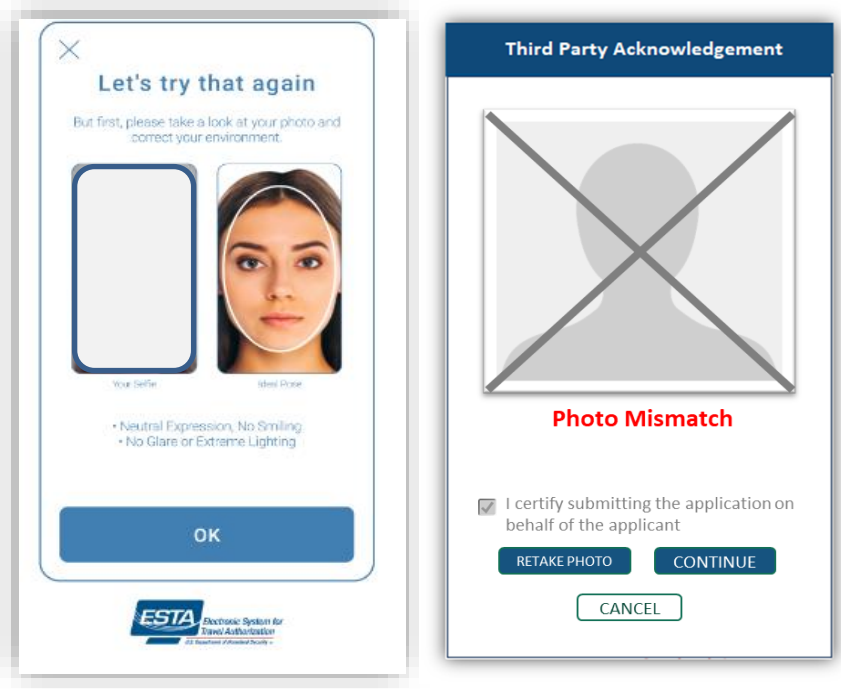

Figure 4: Unsuccessful ESTA Mobile App "selfie" or third-party representative submission

Once the 1:1 biometric verification is complete, the applicant or representative is prompted to complete the remaining questions on the ESTA application. The ESTA mobile application requests the same information that is requested on the ESTA website including: phone number and email address; information about current or previous employer; destination address and point of contact in the United States; social media information (optional); and emergency point of contact information. The applicant or representative must also answer the same Visa Waiver Program eligibility questions regarding communicable diseases, arrests and convictions for certain crimes, history of visa revocation or deportation, and other questions. Prior to submission, the applicant or representative is given the opportunity to review and edit the application. Once complete, the applicant or representative is directed to make a payment via Pay.Gov. When making a payment, the applicant or representative remains in the mobile application, but the payment is routed to Pay.Gov. Once Pay.Gov validates the payment information, the ESTA mobile application displays

[16] The Traveler Verification Service will retain the passport photograph and "selfie" for 14 days from submission.

that payment was successfully submitted. The applicant or representative is then prompted to submit the application to CBP. Like the ESTA website, an applicant or representative cannot submit the application without a payment.

Once 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. All ESTA applications submitted via the ESTA mobile application are stored in the ESTA system along with ESTA applications received via the website. CBP uses this information to vet the ESTA application against select national security and law enforcement databases. As described in DHS/CBP/PIA-006(e) Automated Targeting System, "1.2.1 ATS Biometric Vetting Using Facial Recognition," CBP may conduct biometric vetting on ESTA applications that raise security concerns and require additional review.[17] In these circumstances, CBP uses the photographs supplied by the ESTA applicant to match against an Automated Targeting System gallery of photographs associated with derogatory information. This process is currently an ad hoc process that occurs when an ESTA application raises security concerns. However, CBP is developing an IT solution to automatically vet ESTA application-matched photographs against national security and law enforcement databases through the Automated Targeting System. This solution is expected to be completed by the end of 2023 and will allow CBP to vet photographs the same way that ESTA biographic information is already vetted: automatically. Once the vetting process is complete, the mobile application will display whether an ESTA authorization is approved, not authorized, or pending, as described above.

3. NARA-Approved Retention Schedule

Since the 2016 publication of the ESTA Privacy Impact Assessment, the National Archives and Records Administration (NARA) has approved an ESTA Retention Schedule. CBP retains ESTA records for 15 years in accordance with DAA-0568-2019-0006. This retention schedule allows CBP to address any follow-up inquiries or requests related to the application, including inquiries related to law enforcement, public safety, national security, Freedom of Information Act (FOIA)/Privacy Act of 1974 (PA) matters, or correcting errors in the application.

4. Department of State's List of State Sponsors of Terrorism

The Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015[18] generally makes certain nationals of Visa Waiver Program participating countries ineligible (with some exceptions) from traveling to the United States under the Visa Waiver Program if the

[17] *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(e) (2017). Addendum 1.2.1: ATS Biometric Vetting Using Facial Recognition provides a full explanation of this process, *available at* https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf.
[18] *See* Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015, Pub. L. No. 114-113, Division O, Title II.

applicant is also a national of or has been present in countries designated by the Department of State as a state sponsor of terrorism or any other country or area of concern as designated by the Secretary of Homeland Security. DHS/CBP/PIA-007(e) published on February 17, 2016, listed specific countries that were designated as a state sponsor of terrorism. With this update, CBP is now relying on the Department of State's list of state sponsors of terrorism available at https://www.state.gov/state-sponsors-of-terrorism/. This edit will accommodate future changes, should countries be added to or removed from the list of designated state sponsors of terrorism.

5. ESTA Land

As of October 1, 2022,[19] in accordance with an Interim Final Rule (IFR),[20] Visa Waiver Program travelers entering the United States by land are now required to obtain an approved ESTA authorization. Under this Interim Final Rule, Visa Waiver Program travelers intending to travel to the United States by land must receive an ESTA travel authorization prior to application for admission to the United States. Prior to this, Visa Waiver Program travelers may have used either an approved ESTA or apply for an I-94W to enter the United States. The change on October 1, 2022, requires Visa Waiver Program travelers to obtain an ESTA authorization and pay the I-94 fee prior to arrival.

Privacy Impact Analysis

Authorities and Other Requirements

There are no changes to CBP authorities and other requirements with this Privacy Impact Assessment update. CBP collects this information pursuant to Title IV of the Homeland Security Act of 2002, 6 U.S.C. 201 *et seq.*, the Immigration and Nationality Act (INA), as amended, including 8 U.S.C. 1187(a)(11) and (h)(3), and implementing regulations contained in 8 CFR part 217; the Travel Promotion Act of 2009, Public Law 111-145, 22 U.S.C. 2131. Furthermore, CBP's general law enforcement authorities empower it to gather information, including information found via social media, which is relevant to its enforcement missions.[21]

The DHS/CBP-009 ESTA System of Records Notice (SORN) was updated to account for enhancements to ESTA including collection of this information.[22]

---

[19] *See* https://www.cbp.gov/newsroom/national-media-release/cbp-expands-esta-requirements-visa-waiver-program-travelers.
[20] *See* Implementation of the Electronic System for Travel Authorization (ESTA) at U.S. Land Borders (April 1, 2022), *available at* https://www.federalregister.gov/documents/2022/04/01/2022-06366/implementation-of-the-electronic-system-for-travel-authorization-esta-at-us-land-borders.
[21] *See* 8 U.S.C. 1357(b).
[22] *See* DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 87 FR 41338 (July 12, 2022), *available at* https://www.dhs.gov/system-records-notices-sorns.

ESTA resides within the CBP e-Business Cloud security boundary. The CBP e-Business Cloud Authority to Operate was renewed in September 2020.

Office of Management and Budget (OMB) Control Number 1651-0111 continues to cover the collection of ESTA information under the Paperwork Reduction Act (PRA). CBP concurrently received approval by OMB to amend this collection under the Paperwork Reduction Act.[23]

Characterization of the Information

CBP continues to collect and maintain the information previously outlined in the ESTA Privacy Impact Assessment series. However, the type of information that CBP requests may vary depending on how an applicant or representative chooses to submit their application. For website applications, applicants and representatives now capture or upload a photograph of the passport biographic data page, to include the passport photograph. If the applicant or representative chooses to submit the information through the mobile application, CBP is also collecting the applicant's passport photograph as well as a "selfie." CBP is enabling applicants and representatives to submit a photograph of the passport (ESTA website) or rely on mobile device technology to retrieve biographic and biometric information from the passport (ESTA app). This technology eliminates the need for the applicant or representative to manually input a large amount of the biographic information requested in the ESTA application. This functionality reduces the potential for an applicant or representative to manually enter inaccurate information into the application.

CBP continues to collect information from the same sources, including individual applicants intending to travel under the Visa Waiver Program, as well as representatives (e.g., travel agent, family members). In addition to individual applicants and representatives manually inputting information into the ESTA application, applicants and representatives now also use technology advancements (e.g., optical character recognition, Near Field Communication, and Machine-Readable Zone scans) to populate information into the application.

Privacy Risk: There is risk that applicant or representatives will submit inaccurate information about themself or on behalf of the ESTA applicant.

Mitigation: This risk is partially mitigated. There is always an inherent risk that CBP may receive inaccurate information about applicants, especially through third-party submissions. Although CBP cannot prevent users from submitting inaccurate information on behalf of themselves or other people, CBP is adding the enhancements described above to reduce the potential for an applicant or individual to manually enter inaccurate information into the website.

[23] The 30-day notice for the amendment published on February 24, 2022. *See* https://www.federalregister.gov/documents/2022/02/23/2022-03814/arrival-and-departure-record-nonimmigrant-visa-waiver-arrivaldeparture-electronic-system-for-travel. In this notice, CBP proposed amending the ESTA application to change social media collection from optional to mandatory. However, after further consideration, CBP withdrew this change and provision of social media information by an ESTA applicant remains optional/voluntary.

CBP also provides multiple opportunities for the applicant and representative to verify the information within the ESTA application, both on the ESTA website and mobile application, prior to submission. If erroneous information is entered this will not result in a mandatory denial but may require manual adjudication – and therefore additional time – prior to CBP providing a response back to the applicant. Furthermore, a CBP officer may use the information found during the ESTA vetting process to help inform questioning of the applicant at the port of entry. If an applicant or representative provides information as part of the ESTA authorization that is later found to be inaccurate, the applicant may be subject to a secondary inspection. After submission, ESTA applicants may update their accounts by submitting a new destination address in the United States, carrier, flight number, city of embarkation, email address, or telephone number. Corrections to any other data elements will require the applicant to fill out and submit a new ESTA application. Applicants that are denied authorization to travel to the United States will be directed to a U.S. embassy or consulate to request a visa application. Should inaccuracies be identified in the applicant's information during the visa application process, the State Department will consider that fact in determining eligibility for a visa.

Privacy Risk: There is a risk that CBP is collecting more information than necessary to include the image of the biographic passport page, passport photograph, and "selfie" (for mobile application submissions) to grant travel authorizations.

Mitigation: This risk is partially mitigated. CBP is collecting the passport and selfie photographs to complete a 1:1 biometric identity verification and conduct vetting. The collection of photographs ensures that the individual submitting the application is the passport holder. CBP currently collects photographs from non-citizen individuals upon arrival at a U.S. port of entry for vetting and verification purposes. This timing of the collection through the ESTA application allows CBP to verify identity in advance and conduct certain vetting prior to the traveler's arrival. CBP retains the photograph and "selfie" in the Traveler Verification Service for 14 days after submission. Furthermore, CBP retains the image of the biographic passport page and "selfie" in ESTA, for 15 years, to reference, as needed, in the future and for identity verification and reconciliation purposes.

Privacy Risk: There is a risk that the information populated into the application via optical character recognition, Near Field Communication, and Machine-Readable Zone scans will be inaccurate.

Mitigation: This risk is partially mitigated. Prior to submission of an ESTA application, applicants and representatives are prompted to review the application to confirm that the information is accurate and complete. If data is inaccurately populated into the ESTA application via optical character recognition, Near Field Communication, or the Machine-Readable Zone scan, applicants and representatives are given the opportunity to correct and edit the information prior to submission. Individuals will not have access to their information after submitting their

application. Applicants will be able to see the information they supply on the application as they fill it out and again before submission, to confirm it is timely and accurate. Applicants will not be able to view any data once it has been submitted because the web interface cannot guarantee the person requesting information is authorized to access it. After submission, applicants may update their accounts by submitting a new destination address in the United States, carrier, flight number, city of embarkation, email address, or telephone number. Corrections to any other data elements will require the applicant to fill out and submit a new ESTA application. Applicants that are denied authorization to travel to the United States will be directed to a U.S. Embassy or Consulate to request a visa application. Should inaccuracies be identified in the applicant's information during the visa application process, the State Department will consider that fact in determining eligibility for a visa.

Uses of the Information

CBP is now collecting photographs to verify the identity of the applicant against the photograph on the applicant's passport. The primary purpose of the new photograph collection is for identify verification, however CBP will continue to use all information submitted as part of an ESTA application to determine the eligibility of an applicant to travel to the United States under the Visa Waiver Program and to determine whether the applicant poses a law enforcement or security risk to the United States.[24] CBP will continue to vet the ESTA applicant information, now including photograph, against selected security and law enforcement databases at DHS, including TECS and the Automated Targeting System. Additionally, CBP National Targeting Center (NTC) analysts may continue using the social media information supplied on the application to conduct "Overt Research"[25] and "Masked Monitoring, consistent with DHS and CBP policy."[26] Further, CBP may assess social media information irrespective of whether the ESTA applicant voluntarily provides their social media information. The social media information will be used in the same manner previously described in the DHS/CBP/PIA-007(g).

Privacy Risk: There is a risk that CBP will use the passport and selfie photographs for uses beyond the liveness test and identity verification purposes within the ESTA mobile application.

[24] *See* 8 U.S.C. § 1187(h)(3).
[25] Overt Research means collecting information from social media without logging in or otherwise interacting with individuals through social media. Overt research does not include creating identities or credentials on social media, nor does it include concealing a government affiliation to conduct research or general, operational awareness (e.g., non-DHS affiliated IP address).
[26] Masked Monitoring means using identities or credentials on social media that do not identify a DHS/CBP affiliation, or otherwise concealing a government affiliation, to conduct research or general, operational awareness. Masked monitoring includes logging in to social media but does not include engaging or interacting with individuals on or through social media (which is defined as Undercover Engagement).

Mitigation: This risk is partially mitigated. CBP will only use the photographs as described in this Privacy Impact Assessment. When submitting the ESTA application via the website, CBP requires applicants and representatives to submit the biographic passport data page to include the passport photograph. The purpose of this collection is to reduce the chance of the applicant or representative entering inaccurate biographic information into the application. When an individual submits the ESTA application via the mobile application, CBP collects the biometric photograph from the passport's e-chip and a "selfie" photo. CBP then uses the Traveler Verification Service to conduct a 1:1 comparison of the "selfie" and the biometric passport photograph. The purpose of this comparison is to ensure the individual submitting the application is the same person as the person on the identity documents. The photographs are stored in the ESTA database for 15 years for future identity reconciliation purposes. Additionally, the "selfie" and passport photograph that are sent to the Traveler Verification Service are stored for 14 days for analysis and evaluation purposes. In addition to using the selfie to conduct a liveness test and for identity verification purposes, CBP may also use the selfie to conduct biometric vetting in the future. As described in, DHS/CBP/PIA-006(e) Automated Targeting System, "1.2.1 ATS Biometric Vetting Using Facial Recognition," CBP uses the photograph submitted as part of the ESTA application to conduct biometric vetting. At the time of publication of this Privacy Impact Assessment, biometric vetting occurs on an ad hoc basis when an ESTA application raises security concerns and requires additional manual review. In the future, CBP plans to use the selfie and passport photographs to conduct biometric vetting on all ESTA applications on an automated basis.

Privacy Risk: There is a risk that biometric vetting will result in an inaccurate match to photographs associated with derogatory information.

Mitigation: This risk is partially mitigated. CBP is continually testing and evaluating the accuracy of its facial matching algorithms. If the Automated Targeting System facial recognition technology generates a match on biometric data, but there is no match on any biographic data associated with the photographs, CBP officers are required to manually review and cross reference the relevant records in the Automated Targeting System to improve the level of confidence and reliability of matches made to derogatory information before any adjudication decision is made. CBP uses all available information when making a decision and no adverse action may be taken based solely on the results of facial recognition technology matching.

Notice

CBP is providing notice of these changes through the publication of this Privacy Impact Assessment. Additionally, both the ESTA web application and the mobile application present users with a Privacy Act Statement prior to the collection of information. Additionally, CBP also received OMB approval for photographs through OMB Number 1651-0111 on May 25, 2023, – a process that requires additional measures of notice. There are no new risks to notice.

Data Retention by the Project

Applicants and representatives can start and stop the application at any time. CBP does not begin processing the authorization until the payment is made. While the mobile application does not retain any data, even on a temporary basis, the ESTA system will temporarily retain the data for 7 days in a segregated database that is inaccessible by CBP vetting systems. After 7 days, the data will be destroyed. Upon formal submission, the traveler's application data, the passport photo, and the "selfie" will be stored in the ESTA system. In addition, the Automated Targeting System retains a copy of ESTA application biographic data and vetting results to identify individuals from designated countries participating in the Visa Waiver Program who may pose a security risk. By the end of 2023, CBP plans to include the photographs in the transmission of data from ESTA to the Automated Targeting System. Finally, photographs are stored in the Traveler Verification Service for 14 days.

Since the publication of DHS/CBP/PIA-007(g), NARA has approved an ESTA Retention Schedule. CBP retains ESTA records for 15 years in accordance with DAA-0568-2019-0006. This retention schedule allows CBP to address any follow-up inquiries or requests related to the application, including inquiries related to law enforcement, public safety, national security, Freedom of Information Act/Privacy Act matters, or correcting errors in the application.

Information Sharing

CBP will continue to share ESTA application information, including the biometric and selfie photographs, with other federal government authorities, including Intelligence Community partners (e.g., the National Counterterrorism Center), and CBP may share ESTA information on a case-by-case basis to appropriate state, local, tribal, territorial, or international government agencies.

Privacy Risk: There is a risk of CBP sharing biometric information, including the photographs, improperly with external partners.

Mitigation: This risk is partially mitigated. There is an inherent risk to sharing information, including biometric information, with partner agencies. However, absent any legal prohibitions, CBP may share information from the ESTA application, including biometric information, with other external partners who have an authorized purpose to access the information in performance of their duties, possess the requisite security clearance (if applicable), and assure adequate safeguarding and protection of the information. CBP carefully reviews and evaluates the sharing prior to disclosure of information to an external partner. Disclosure of biometric information obtained from the ESTA application must be compatible with the purposes for which the data was collected and authorized under the Privacy Act of 1974, 5 U.S.C. § 552a(b)(3), specifically the routine uses set forth in the ESTA and Automated Targeting System System of Records Notices or as otherwise permitted by the Privacy Act. Additionally, for ongoing, systematic sharing, CBP completes an information sharing and

access agreement with external partners to establish the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy safeguards for the data.

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. No information is stored locally on the user's device or in the ESTA mobile application itself. CBP retains all ESTA application data within the ESTA system, which is subject to the system's security controls. A copy of the biographic information and vetting results is also available in Automated Targeting System which is subject to that system's security controls. Additionally, CBP has analyzed the mobile application to ensure that information is sent only to CBP, and the application can only access the information necessary to complete the functions.

Contact Official

Matthew Davies
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

Approval Signature

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

_____

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