Privacy Impact Assessment Update
for the

Electronic System for Travel Authorization (ESTA)

DHS/CBP/PIA-007(g)

September 1, 2016

Contact Point
Suzanne Shepherd
Director - ESTA
U.S. Customs and Border Protection
(202) 344-3710

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Electronic System for Travel Authorization (ESTA) is a web-based 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 update to the Privacy Impact Assessment (PIA) for ESTA, last updated on June 20, 2016, to provide notice and assess the privacy risks associated with recent enhancements to the ESTA application questionnaire, including the addition of an optional field for social media usernames or identifiers for all ESTA applicants.

Overview

ESTA is a web-based system designed to determine foreign nationals' eligibility to travel to the United States under the VWP. Applicants use the ESTA website to submit biographic information and respond to questions related to an applicant's eligibility to travel under the VWP. ESTA information is necessary to issue a travel authorization, consistent with the requirements of the Form I-94W.[2] A VWP traveler who intends to arrive at a U.S. air or sea port of entry must obtain an approved travel authorization via the ESTA website prior to boarding a carrier bound for the United States. The ESTA program allows CBP to eliminate the requirement that VWP travelers complete a Form I-94W prior to being admitted to the United States via an air or sea port of entry because the ESTA application electronically captures duplicate biographical and travel data elements collected on the paper Form I-94W.

DHS/CBP published an ESTA PIA update on June 20, 2016,[3] in accordance with the new requirements of the Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015.[4] In that update, DHS/CBP addressed new eligibility requirements established by the Act to strengthen the security of the VWP to appropriately meet the current threat environment to the United States.

---

[1] *See* 8 CFR § 217. The Visa Waiver Program (VWP), administered by the Department of Homeland Security (DHS) in consultation with the Department of State, permits citizens of 38 countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those 38 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* 8 CFR § 217.5(c). The Form I-94W must be completed by all nonimmigrant visitors not in possession of a visitor's visa who are nationals of one of the VWP countries enumerated in 8 CFR § 217.
[3] *See* DHS/CBP/PIA-007 Electronic System for Travel Authorization (ESTA), and subsequent updates, *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-esta-june2016_0.pdf.
[4] *See* Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015, Pub. L. No. 114-113, Division O, Title II.

Reason for the PIA Update

DHS/CBP is updating the ESTA questionnaire with the following enhancements: including an optional field in which ESTA applicants may include information about their presence on select social media platforms.

Social Media Identifiers

DHS/CBP is expanding the ESTA application to request social media identifiers from all ESTA applicants. DHS/CBP will use social media identifiers to conduct screening, vetting, and law enforcement checks of ESTA applicants using publicly available information on social media. Terrorist groups, including the Islamic State of Iraq and the Levant (ISIL), al-Qa'ida, and al-Qa'ida's affiliates actively use open media (social media, specifically) to disseminate official messaging, recruit potential members, and convince potential supporters to mobilize to violence. Adding such a question to the ESTA application will provide DHS with greater opportunities to inform a determination of eligibility for travel to the United States.

While this field is optional, all information submitted may be used for national security and law enforcement vetting purposes, and for VWP eligibility determinations. Should an individual choose to provide his or her social media identifier(s), and an initial screening by DHS/CBP indicates possible information of concern, DHS/CBP may use tools and search techniques in an attempt to locate and positively identify social media accounts and profiles belonging to the applicant. DHS/CBP Officers already use publicly available information, including social media information, as part of the existing ESTA screening and vetting processes. Under no circumstance will DHS/CBP violate any social media privacy settings in the processing of ESTA applications.

The inclusion of social media identifiers on the ESTA application is the first time that DHS has requested social media information as part of an application for benefits or travel to the United States. Due to the novel privacy risks surrounding this information collection, the DHS Privacy Office requires additional privacy risk mitigation strategies to evaluate this information collection:

a) The collection of social media identifiers will be used to determine the data quality, integrity, and use(s) of the information;
b) DHS/CBP will brief the DHS Social Media Task Force on this collection and its operational outcomes;
c) The DHS Social Media Task Force will review the results of the collection to evaluate the effectiveness of the questions in combatting the national security threat.
d) The DHS Privacy Office will initiate a Privacy Compliance Review (PCR) of the DHS/CBP collection and use of social media information for ESTA applicant vetting six months after DHS/CBP begins collecting social media information.

Privacy Impact Analysis

Authorities and Other Requirements

No change from the previously published ESTA PIA update.

Characterization of the Information

CBP is expanding the ESTA data elements to include social media provider/platform, and social media identifier or username.

Privacy Risk: There is a risk that individuals, who do not use social media, will input the social media account information of a family member or associate in the ESTA application.

Mitigation: This risk is partially mitigated. The ESTA application instructs applicants that social media fields are optional. If an applicant chooses to not fill out or answer questions regarding social media the ESTA application can still be successfully submitted. There is no indication that an applicant should enter information of family members or associates.

Privacy Risk: There is a risk of inappropriate collection of First Amendment protected information, as regulated by the Privacy Act, 5 U.S.C. § 552a(e)(7). CBP may collect records that it is restricted from maintaining under subsection (e)(7) of the Privacy Act, which prohibits maintaining records that describe how individuals exercise their First Amendment rights.

Mitigation: While there is a risk of this collection, the collection is pertinent to, and within the scope of, authorized CBP law enforcement activity[5]. The application will specify that this information is optional, so no applicant will be required to provide any information regarding social media. In addition, there remains the possibility that some other information within the scope of subsection (e)(7)—either content shared by the applicant following admission into the United States or content from others, such as U.S. citizens, appearing within the applicant's social media profile—may be collected during the vetting process. While the information may be used to make an admissibility determination, DHS/CBP does not intend to maintain such third-party information as part of the ESTA application, and any such collection will be within the scope of an authorized law enforcement activity, as permitted by subsection (e)(7).

Privacy Risk: CBP may make determinations about ESTA applicants based on inaccurate information posted on social media.

Mitigation: This risk is partially mitigated. Information is collected directly from

[5] *See* 5 U.S.C. § 552a(e)(7).

applicants, and individuals generally have some degree of control over what is posted on their social media account. CBP presumes some of this information is accurate. However, information posted by an associate of the applicant on the applicant's social media page may also be taken into consideration. Information collected from social media, by itself, will not be a basis to deny someone entry to the United States. CBP will also develop procedures and training focused on understanding data quality limitations associated with social media. In addition, if an individual is denied travel via ESTA, he or she is still eligible to apply for a visa from the U.S. Department of State.

Privacy Risk: CBP may collect information about other individuals who may have posted or interacted with the ESTA applicant on his or her publicly facing social media platform(s).

Mitigation: This risk is partially mitigated. CBP will view information about individuals who are associated with an applicant's social media account. However, CBP will not retain information unless it is relevant to making an ESTA determination.

Uses of the System and the Information

DHS/CBP will use social media identifiers to conduct screening, vetting, and law enforcement checks of ESTA applicants from publicly available information on social media. Use of publicly available information on social media platforms to make an eligibility determination for an ESTA applicant complied with DHS Management Directive 110-01-011 "Privacy Policy for Operational Use of Social Media," and was approved by the DHS Privacy Office for certain offices within CBP.

Users within the CBP National Targeting Center (NTC) may engage in social media information collection using both "Overt Research" and "Masked Monitoring." The CBP Directive on the Operational Use of Social Media defines Overt Research and Masked Monitoring as follows:

- 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).
- 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).

Only approved CBP users from the NTC, who have signed social media rules of behavior and completed mandated privacy training for the operational use of social media, may participate in the collection of information about ESTA applicants from social media platforms. These NTC users may deviate from the DHS standard social media rules of behavior (pursuant to MD 110-01-011) to conduct Masked Monitoring of publicly available social media sites. CBP users from the NTC may deviate from the requirement to use online screen names or identities that indicate an official DHS affiliation and use DHS email addresses to open accounts when using social media in the performance of their duties. However, these users must still respect online privacy settings and may not interact (e.g., friend, fan, like, or message) with social media users.

CBP will continue to use all of the information submitted as part of an ESTA application to determine the eligibility of an applicant to travel to the United States under the VWP and to determine whether the applicant poses a law enforcement or security risk to the United States.[6] CBP will continue to vet the ESTA applicant information against selected security and law enforcement databases at DHS, including TECS[7] (not an acronym) and the Automated Targeting System (ATS).[8]

CBP will retain information from social media platforms collected during the vetting of an ESTA application in ATS. Though the information collected will largely pertain to user accounts operated by the individual that submitted the ESTA application, it is possible that information belonging to the applicant's social media contacts will be captured. Through link-analysis, CBP may identify direct contacts (such as an ESTA applicants "friends," "followers," or "likes"), as well as secondary and tertiary contacts associated with the applicant that pose a potential risk to the homeland or demonstrate a nefarious affiliation on the part of the applicant. Information related to each of these contacts may be retained in ATS, and used as part of the vetting process.

Privacy Risk: There is a risk that CBP will inappropriately access information that is not publicly available.

Mitigation: CBP respects the individual's privacy settings on his or her account. All authorized CBP social media users must sign rules of behavior that explicitly prohibit them from accessing private information. Authorized users must also complete privacy training for the operational use of social media.

Privacy Risk: There is a risk that CBP will consider an applicant's failure to complete this optional data element as indicative of potentially derogatory information.

Mitigation: The ESTA application contains language indicating that the social media

[6] *See* 8 U.S.C. § 1187(h)(3).
[7] DHS/CBP-011 U.S. Customs and Border Protection TECS (73 Fed. Reg. 77778, December 19, 2008).
[8] DHS/CBP-006 Automated Targeting System (77 Fed. Reg. 30297, May 22, 2012).

fields are optional. If an applicant elects to not answer questions regarding social media, the ESTA application can still be successfully submitted, and the individual will not be penalized.

Data Retention by the Project

The CBP retention period for ESTA has not changed. CBP retains ESTA application data for no more than three years in an active database (one year beyond the ESTA authorization expiration date) and twelve years in archive status.

However, for information collected from social media sources, CBP must document the date, site(s) accessed, information collected, and how it was used, as with any other CBP information collection.

Privacy Risk: There is a risk that CBP will retain social media information that has no use or value to CBP missions or ESTA eligibility determinations.

Mitigation: All authorized CBP social media users complete privacy training. Only information that has use and value to CBP missions or ESTA eligibility determinations will be retained. CBP will not retain information that is not relevant to the ESTA determination.

The DHS Privacy Office will review these retention practices during the ESTA social media privacy compliance review.

Internal Sharing and Disclosure

No changes have been made to internal sharing and disclosure.

External Sharing and Disclosure

No changes have been made to external sharing and disclosure. CBP will continue to share ESTA information in bulk with other federal Intelligence Community partners (e.g., the National Counterterrorism Center), and CBP may share ESTA data on a case-by-case basis to appropriate state, local, tribal, territorial, or international government agencies. Existing external information sharing and access agreements will continue and will now include the expanded categories or records noted above.[9]

[9] This sharing takes place after CBP determines that the recipient has a need to know the information to carry out functions consistent with the exceptions under the Privacy Act of 1974, 5 U.S.C. § 552a(b), and the routine uses set forth in the ESTA SORN. Additionally, for ongoing, systematic sharing, CBP completes an information sharing and access agreement with federal partners to establish the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy protections for the data.

Notice

The online ESTA application contains a Frequently Asked Questions (FAQ) section that will address the addition of social media elements to the ESTA application. In addition to the FAQs on the online application, there will be a question mark indicator next to social media field(s) that an applicant can click on, which will provide additional information regarding the collection of social media information.

The System of Records Notice (SORN) for ESTA, last published on June 17, 2016, is being updated concurrently with this PIA to reflect the ESTA enhancements of an additional data element on the ESTA application.

Privacy Risk: A risk remains that friends, family members, associates, or affiliates of the ESTA applicant will not be aware of their inclusion on the ESTA application or their exposure to CBP vetting of the ESTA application. This risk expands to include associates or affiliates who interact with the ESTA applicant on his or her social media accounts.

Mitigation: This risk is partially mitigated. The publication of the updated ESTA SORN in the Federal Register will provide general notice that optional social media information may be collected. Additionally, the publication of this PIA expands the notice regarding the possibility of social media information collection on the ESTA application. However, individuals who are not the applicant will not receive direct notice of the collection in a manner similar to the ESTA applicant. There will be an FAQ section on the ESTA application that explains to applicants the inclusion of the optional social media information collection.

Individual Access, Redress, and Correction

No changes have been made to individual access, redress, and correction. The ESTA enhancements will result in CBP denying some individuals eligibility for a travel authorization under the VWP. Applicants denied a travel authorization to the United States via ESTA may still apply for a visa from the U.S. Department of State. General complaints about treatment can be made to the DHS Traveler Redress Inquiry Program (DHS TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Generally, if a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries should be directed to:

CBP INFO Center
OPA - CSC - Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Ave, NW
Washington, D.C. 20229

In addition, CBP has updated the address to which individuals should submit their requests for access and correction. Under the Privacy Act and the Freedom of Information Act (FOIA), individuals may request access to the information they provide that is maintained in the applicable CBP system of records. Proper written requests under the Privacy Act and FOIA should be addressed to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, D.C. 20002

Requests for access should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by CBP. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Technical Access and Security

No changes have been made to technical access or security.

Technology

The inclusion of social media identifiers on the ESTA application is the first time that DHS has requested social media information as part of an application for benefits or travel to the United States. Due to the novel privacy risks surrounding this information collection, the DHS Privacy Office requires additional privacy risk mitigation strategies to evaluate this information collection:

a) The collection of social media identifiers will be used to determine the data quality, integrity, and use(s) of the information;
b) DHS/CBP will brief the DHS Social Media Task Force on this collection and its operational outcomes;
c) The DHS Social Media Task Force will review the results of the collection to evaluate the effectiveness of the questions in combatting the national security threat;
d) The DHS Privacy Office will initiate a Privacy Compliance Review (PCR) of the DHS/CBP collection and use of social media information for ESTA applicant vetting

six months after DHS/CBP begins collecting social media information.

Responsible Official

Suzanne Shepherd, Director ESTA
U.S. Customs and Border Protection
Department of Homeland Security

Debra L. Danisek, Acting CBP Privacy Officer
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security