



Privacy Impact Assessment Update
for the

Electronic Secured Adjudication Forms
Environment (e-SAFE)

DHS/CBP/PIA-057(a)

April 27, 2020

Contact Point

Melanie Mataxas

Admissibility Review Office

Office of Field Operations

(571) 468-1816

Reviewing Official

Dena Kozanas

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

U.S. Customs and Border Protection (CBP) is tasked with determining the admissibility of all individuals seeking admission into the United States. e-SAFE is a web-based waiver application system that allows inadmissible visa-exempt individuals to apply for a waiver of inadmissibility. CBP is updating this Privacy Impact Assessment (PIA) to meet the guidelines contained in Executive Order (EO) 13780, “*Protecting the Nation from Foreign Terrorist Entry into the United States.*” The EO requires the capture of social media “handles” or identifiers of applicants and the names and addresses of individuals with whom waiver applicants anticipate they will be in contact while in the United States. This information will help improve the screening and vetting protocols and procedures associated with the waiver issuance process.

Overview

Individuals who are seeking admission as non-immigrants, but are inadmissible, can file a request for a waiver of inadmissibility. Many travelers seeking admission as non-immigrants will apply for waivers as part of the visa issuance process. Visa-exempt citizens of Canada, Palau, the Federated States of Micronesia, and the Republic of the Marshall Islands who are ineligible to enter the United States due to a ground of inadmissibility must apply for a waiver of ineligibility from CBP’s Admissibility Review Office (ARO).

On July 1, 2019, CBP launched e-SAFE to streamline the adjudication of:

- Form I-192 Application for Advance Permission to Enter as a Nonimmigrant,¹ which is submitted at ports of entry by inadmissible nonimmigrant aliens already in possession of appropriate documents.²
- Form I-212 Application for Permission to Reapply for Admission Into the United States After Deportation or Removal, which is for particular inadmissible immigrants and nonimmigrants who are seeking permission to reapply for admission into the United States (also known as “consent to reapply”)³ after they have been excluded, deported, or removed from the United States⁴ or were unlawfully present in the United States for

¹ The form I-192 is owned by U.S. Citizenship and Immigration Services (USCIS) and available electronically at www.uscis.gov. This form may also be used to apply for T nonimmigrant status and for U nonimmigrants status; however, CBP does not adjudicate T and U nonimmigrant statuses. T and U nonimmigrant statuses are adjudicated by USCIS.

² CBP can grant discretionary relief pursuant to § 212(d)(3)(A) of the INA.

³ Per § 212(a)(9) of the INA.

⁴ Pursuant to § 212 (a)(9)(A) as stipulated in 8 CFR § 212.2 or 212(d)(3)(A).



an aggregate period of more than one year and subsequently entered or attempted to reenter the United States without being admitted.⁵

- Form I-824 Application for Action on an Approved Application or Petition, which is used by nonimmigrant aliens to request a duplicate approval of an approved application or petition made on Forms I-192 and I-212 in cases in which an applicant has lost a copy of his or her original waiver.

The ARO is CBP's centralized office for rendering decisions regarding the adjudication of waivers for previously inadmissible, visa-exempt citizens of Canada, Palau, the Federated States of Micronesia, and the Republic of the Marshall Islands who complete Form I-192, Form I-212, and Form I-824. e-SAFE electronically collects information from visa-exempt citizens of such countries who are eligible to apply for temporary and permanent waivers of inadmissibility. Individuals wishing to obtain a waiver can log into e-SAFE to electronically fill out the required forms and provide the documents required for ARO to make a waiver determination. Paper-based applications for a waiver are available at ports of entry.

Reason for the PIA Update

Executive Order (EO) 13780, "*Protecting the Nation from Foreign Terrorist Entry into the United States*," directs the implementation of a uniform baseline of screening and vetting standards and procedures, which requires the proper collection of all information necessary for a rigorous evaluation of all grounds of inadmissibility or bases for the denial of other immigration benefits.⁶ In a review of information collected for admission and benefit decisions, DHS identified the need to collect social media identifiers ("handles") and their associated social media platforms from applicants to enable and inform identity verification, national security screening and vetting, and related inspections.⁷ In accordance with this EO, DHS also identified the need to collect the names and addresses of the individuals with whom an applicant plans on being in contact while in the United States.

Consistent with the requirement for a uniform baseline of vetting standards described in EO 13780, DHS intends to collect standard data from applicants on immigration and foreign traveler forms and information collection systems. CBP and USCIS will collect social media handles to assess an alien's eligibility to receive an immigration-related benefit from CBP or

⁵ § 212(a)(9)(C) of the INA.

⁶ See 82 FR 13209 (Mar. 6, 2017).

⁷ Vetting, for purposes of immigration enforcement and border security, involves the review and evaluation of information associated to an individual to validate identity, identify potential threats, and identify issues related to fraud, misrepresentation, national security, border security, homeland security, public safety, or law enforcement interests of the United States.



USCIS.

DHS currently uses publicly available social media information to support its vetting and adjudication programs and to supplement other information and tools that DHS trained personnel regularly use in the performance of their duties.⁸ This process includes a labor-intensive step to identify social media handles that can correctly be associated with the applicant. The collection of applicants' social media identifiers and associated platforms will provide DHS adjudication personnel the ability to view publicly available information⁹ on the platforms provided by the applicant and more easily verify that the accounts do belong to an applicant.

Social media may help distinguish individuals of concern from applicants whose information substantiates their eligibility for travel or an immigration benefit. Social media can provide positive, confirmatory information or support a beneficiary's or traveler's application, petition, or claims. It can also be used to identify potential deception, fraud, or previously unidentified national security or law enforcement concerns, such as when criminals and terrorists have provided otherwise unavailable information via social media that identified their true intentions, including support for terrorist organizations.

CBP is not requesting passwords as part of this collection. Applicants who participate in multiple online platforms will provide all handles or other identifiers used for these platforms. The lack of a social media account alone will not affect an applicant's ability to obtain a waiver. Applicants for CBP and USCIS benefits must certify on the respective forms that the information submitted is true and correct to the best of the applicant's knowledge and belief.

USCIS is also updating Forms I-192 and I-212 to include information related to U.S. contacts, including the names, addresses, and telephone numbers of individuals in or outside the United States. For many applicants this information may just be the contact information for a hotel. However, some applicants will provide contact information for actual individuals and their residences. CBP will only review and vet this information in rare circumstances where they have identified issues in an application and need to investigate contacts to determine if the applicant is

⁸ Publicly available social media means the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact, and that has been published or broadcast in some manner to the general public, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available social media does not require a user to purchase or otherwise pay for a subscription of use and does not require an invitation from a user to join or the establishment of a relationship (e.g., "friend," "follow," "connect") to otherwise access information. Publicly available social media may require a user to create an account in order to access services and related content. Social media take many forms, including but not limited to web-based communities and hosted services, social networking sites, and video and photo sharing technologies.

⁹ Publicly available information is unclassified information that has been published or broadcasted in some manner to the general public, is available to the public by subscription or purchase, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.



providing accurate information. CBP may use this information to identify information that would make an applicant ineligible for a waiver. For example, if CBP finds information while researching the U.S. contact that shows that the applicant intends to work while in the United States, a waiver may be denied.

CBP will not vet social media or U.S. contact information unless there is information found from the normal CBP vetting process that raises concerns. If necessary, CBP will use the information, as with all information provided during a waiver application, to determine the approval or denial of a waiver application. Collecting this additional information from waiver applicants will strengthen the process for vetting applicants and confirming their identity.

CBP is conducting this PIA update to provide notice of its compliance with the new EO and describe its implementation of the requirement to include social media handles and U.S. contact information on forms submitted to CBP via e-SAFE. This PIA update describes the collection and uses of the new information CBP receives from applicants via e-SAFE who are applying for a waiver using Forms I-192 and I-212 as mandated by EO 13780 and the subsequent Presidential implementing memorandum.¹⁰

Privacy Impact Analysis

Authorities and Other Requirements

There is no change in authorities from the previously published e-SAFE PIA other than the new Executive Order, EO 13780 “Protecting the Nation from Foreign Terrorist Entry into the United States.”

Characterization of the Information

DHS is updating Form I-192 to collect social media handles and the name of the associated social media platforms used by an applicant during the past five years. DHS is seeking this information in addition to existing information consistent with other U.S. Government data collections for immigrant and nonimmigrant visas. DHS will not collect social media passwords.

¹⁰ See Memorandum for the Secretary of State, the Attorney General, and the Secretary of Homeland Security Implementing Immediate Heightened Screening and Vetting of Applications for Visas and Other Immigration Benefits, Ensuring Enforcement of All Laws for Entry Into the United States, and Increasing Transparency Among Departments and Agencies of the Federal Government and for the American People, *available at* <https://www.federalregister.gov/documents/2017/04/03/2017-06702/implementing-immediate-heightened-screening-and-vetting-of-applications-for-visas-and-other>.



Additionally, DHS is updating Form I-192 and Form I-212 to include name, telephone number, and address for an applicant's point of contact in the United States.

Waiver applicants use e-SAFE to complete and submit the forms for review and adjudication by CBP. CBP does not review these new data elements unless concerns arise during the regular review process. Applicants are able to respond "none" to the questions asking about social media handles. Applicants are required to affirm that the information they provide is accurate. The lack of a social media account alone will not affect an applicant's ability to obtain a waiver.

Privacy Risk: There is a risk that CBP is collecting more information than is necessary to adjudicate admissibility waivers.

Mitigation: This risk is partially mitigated. CBP does not own or control the forms used to adjudicate admissibility waivers. USCIS controls the forms and updated the forms in accordance with an EO. Although CBP may not necessarily view and vet social media identifiers and U.S. contact information for all waiver applicants, that information will assist CBP in adjudicating some applications. If, during the course of its regular adjudication of waivers, CBP identifies area(s) of concern, then CBP may seek to identify publicly available information associated with the waiver applicant and/or to investigate U.S. contacts listed by an applicant. CBP will use the provided social media identifiers and U.S. contact information to streamline their vetting of the waiver applicant.

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

Mitigation: This risk is partially mitigated. The application instructs applicants to provide their social media handle and informs them that CBP will use that information when processing the application. DHS currently uses publicly available social media information to support its vetting and adjudication programs, which CBP trained personnel regularly use in the performance of their duties. This process includes will include steps to validate that the identified social media is correctly associated with the applicant prior to making adjudication decisions. CBP does not mandate that applicants provide their social media handle nor the account of a family member or a friend in order to submit form I-192 electronically via e-SAFE or on paper. Additionally, CBP does not view the activity on all social media accounts provided by an applicant.

Privacy Risk: There is a risk of collection of protected information, as regulated by the Privacy Act of 1974, 5 U.S.C. § 552a. CBP may collect records that are restricted under 5 U.S.C. § 552a(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 collection of protected information, the collection is pertinent to, and within the scope of, CBP's authorized law enforcement activity.¹¹ While the information may be used along with other information to make an admissibility determination, CBP does not intend to maintain such third-party information as part of the application, and any such collection will be within the scope of an authorized law enforcement activity, consistent with subsection (e)(7) of the Privacy Act.

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

Mitigation: This risk is partially mitigated. Applicants directly submit information to CBP via e-SAFE, and individuals generally have some degree of control over what is posted on their social media accounts. CBP presumes that this information is accurate; however, CBP may take into account information posted by an associate of the applicant on the applicant's social media when making an adjudication. Information collected from social media, by itself, will not be a basis to approve or deny an applicant a waiver. CBP will also develop procedures and focus training on understanding data quality limitations associated with social media. In addition, if CBP denies an applicant's waiver, he or she may still appeal the decision with the Board of Immigration Appeals.

Privacy Risk: CBP may collect information about other individuals who may have posted or interacted with a waiver 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 a determination on the application.

Uses of the Information

CBP may use social media identifiers to conduct screening, vetting, and law enforcement checks of waiver applicants using publicly available information on social media. These checks will only occur if the normal CBP review process identifies areas of concern in an application. CBP will not specifically vet U.S. contacts listed on an application but may conduct research if concerns arise during the normal ARO process, and it is believed that resolution can be resolved by researching the U.S. contacts submitted by the applicant. CBP may conduct research by running information through CBP holdings or by using publicly available information. CBP will collect this data from the admissibility waiver forms that applicants submit through e-SAFE. This collection of information is necessary to enable DHS to assess an alien's eligibility to travel to or

¹¹ See 5 U.S.C. § 552a(e)(7).



be admitted to the United States or to receive an immigration-related benefit from DHS.

Social media may help distinguish individuals of concern from applicants whose information substantiates their eligibility for travel or an immigration benefit. Social media can provide positive, confirmatory information or support a beneficiary's or traveler's application, petition, or claims. It can also be used to identify potential deception, fraud, or previously unidentified national security or law enforcement concerns.

DHS personnel will review information on social media platforms in a manner consistent with the privacy settings the applicant has chosen to adopt for those platforms. Only that information which the account holder has allowed to be shared publicly will be viewable by DHS.

CBP will continue to use all of the information submitted as part of a waiver application to render a decision and to determine whether the applicant poses a law enforcement or security risk to the United States.¹² CBP will continue to vet submitted waiver applicant information against selected security and law enforcement databases at DHS, including TECS¹³ and the Automated Targeting System (ATS).¹⁴ This includes social media and U.S. contact information.

CBP may retain information from social media platforms during the vetting of a waiver application in ATS. Though the information collected will largely pertain to user accounts operated by the individual who submitted the waiver application, it is possible that CBP will capture information belonging to the applicant's social media contacts. Through link-analysis, CBP may identify direct contacts (such as an I-192 applicant's "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. CBP may retain information related to each of these contacts in ATS and then use that information as part of the vetting process.

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

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

¹² See 8 U.S.C. § 1187(h)(3).

¹³ 7 DHS/CBP-011 U.S. Customs and Border Protection TECS (73 Fed. Reg. 77778, December 19, 2008).

¹⁴ 8 DHS/CBP-006 Automated Targeting System (77 Fed. Reg. 30297, May 22, 2012).



Privacy Risk: There is a risk that CBP will consider an applicant's failure to complete the social media data element fields as indicative of potentially derogatory information being present on social media.

Mitigation: If an applicant selects none for no social media handle/accounts or does not answer questions regarding social media, the waiver application can still be successfully submitted, and the individual will not be penalized for not having a social media account.

Notice

For waiver applicants using e-SAFE, CBP provides notice at the time of collection. The e-SAFE electronic application contains a Frequently Asked Questions (FAQ) section that will address the addition of social media elements to the electronic application. In addition to the FAQs on the online application, there will be a question mark indicator next to social media field(s) on which an applicant can click, which will provide additional information regarding the collection of social media information. This PIA serves as notice to third parties whose information an applicant may provide as part of the waiver application process.

Privacy Risk: A risk remains that friends, family members, associates, or affiliates of the waiver applicant will not be aware of their inclusion on the e-SAFE electronic application or their exposure to CBP vetting of the application. This includes U.S. citizens and foreign associates or affiliates who publicly interact with the waiver applicant on his or her social media accounts, as well as U.S. citizens who may be listed as a point of contact.

Mitigation: This risk is partially mitigated. The publication of this PIA expands the notice regarding the possibility of social media information collection and the inclusion of U.S. point of contact information on the waiver application. There will be a FAQ section on the e-SAFE website and CBP.GOV that explains to applicants the social media information collection process. CBP cannot view any private interactions individuals make on social media.

Data Retention by the Project

The CBP retention period for e-SAFE application has not changed. e-SAFE retains information actively for 5 years and in archives for 12 additional years. This includes complete and incomplete applications. CBP retains information submitted through e-SAFE to vet prospective travelers seeking to enter the United States. CBP continuously vets information for the life of the waiver, 5 years after an applicant is admitted into the United States. Information will be kept in archives for 12 years to allow retrieval of the information for law enforcement and investigatory purposes.



DHS retains information that is included in an individual's official A-File permanently, consistent with the A-File SORN. The official A-File record may take three possible forms: (1) records contained within the paper A-File; (2) records contained within the electronic record from the Enterprise Document Management System¹⁵ or USCIS Electronic Immigration System;¹⁶ or (3) a combination of paper and electronic records and supporting documentation. DHS maintains A-File records in accordance with N1-566-08-11. DHS/USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth.

Information Sharing

CBP has made no changes to the sharing and disclosure of information out of e-SAFE. CBP will continue to share waiver information in bulk with federal Intelligence Community partners (e.g., the National Counterterrorism Center), and CBP may share I-192 waiver application 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.¹⁷

Redress

CBP has made no changes to individual access, redress, and correction.

Auditing and Accountability

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 will participate in the collection of information about waiver applicants from social media platforms. CBP complies with DHS approved directives and policies when using publicly available information on social media platforms to make a determination for a waiver applicant. CBP users are required

¹⁵ See DHS/USCIS/PIA-003(b) Integrated Digitization Document Management Program, *available at* www.dhs.gov/privacy.

¹⁶ See DHS/USCIS/PIA-056 USCIS Electronic Immigration System, and subsequent updates, *available at* www.dhs.gov/privacy.

¹⁷ 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). 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.



to document any time they use social media for an operational use, including keywords searched and social media sites accessed. If necessary, CBP can access audit logs that show the websites and searches used while conducting research on waiver applicants.

Responsible Officials

Guy Cangé
Office of Field Operations
U.S. Customs and Border Protection
571-468-6704

Debra L. Danisek
CBP Privacy Officer
Office of Privacy and Diversity
U.S. Customs and Border Protection
202-344-1610

Approval Signature

[Original signed and on file with the DHS Privacy Office]

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security