Privacy Impact Assessment

for the

Electronic Visa Update System

DHS Reference No. DHS/CBP/PIA-033(a)

May 18, 2023

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Electronic Visa Update System (EVUS) is a web-based enrollment system that collects information and updates from certain nonimmigrant aliens in advance of their travel to the United States. Enrolling with EVUS is a requirement for certain individuals traveling to the United States for temporary business or tourism using certain visa types. CBP is publishing this Privacy Impact Assessment update to provide notice and to assess the privacy risks associated with recent modifications to the EVUS application questionnaire, including the addition of an optional social media field on EVUS applications.

Overview

Every individual seeking admission to the United States as a nonimmigrant[1] must establish that they are admissible to the United States.[2] Upon arrival at a United States port of entry (POE), nonimmigrants are typically required to present a valid passport, a travel and identity document issued by the traveler's country of citizenship, and valid visa, a document placed in the passport signifying that the United States has given the individual permission to enter the country for a specific period of time. In certain circumstances, such as under the Visa Waiver Program,[3] one or both of these document requirements can be waived.[4] A nonimmigrant's travel purpose (e.g., tourism, business) determines for which type of visa an individual may apply.[5] The nonimmigrant visa application process generally requires the individual to fill out an application, pay a visa application fee, and appear for an interview before a consular officer at a U.S. embassy or consulate.

Every visa applicant undergoes extensive security checks before a visa is issued. At the U.S. embassy or consulate, officials review the application, collect the applicant's fingerprints, and check the applicant's name against government systems and watchlists. The consular officer generally interviews the visa applicant and reviews his or her application and supporting documents. When all required processing is completed, and if the applicant is found eligible, the

[1] The term nonimmigrant refers to foreign nationals who are admitted to the United States temporarily for a specific purpose. By contrast, the term immigrant refers to foreign nationals who wish to come to the United States permanently.
[2] *See* INA §§ 235(b)(2)(A), 291, 8 U.S.C. §§ 1225(b)(2)(A), 1361; 8 CFR §§ 214.1(a)(3), 235.1(f), 235.3.
[3] The Visa Waiver Program (VWP), administered by the Department of Homeland Security (DHS) in consultation with the State Department, permits citizens of 39 countries to travel to the United States for business or tourism for stays of up to 90 days without a visa. In return, those 39 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.
[4] *See* INA § 212(a)(7)(B), 8 U.S.C. § 1182(a)(7)(B); 8 CFR § 212.1; *see also* INA § 217, 8 U.S.C. § 1187; 8 CFR § 217.
[5] *See* INA § 101(a)(15), 8 U.S.C. § 1101(a)(15) (defining nonimmigrant classifications); *see also* U.S. Department of State, Bureau of Consular Affairs, "Directory of Visa Categories" (listing visa categories).

consular officer issues a nonimmigrant visa. The validity period of a U.S. nonimmigrant visa may vary by category and may vary considerably, including for extended periods of up to ten years and multiple entries.[6] When the visa validity period expires, if the individual plans to travel to the United States, they must renew their visa. The process is generally the same whether a person is applying for a visa for the first time or renewing an expired visa. This means that to renew a visa the individual must submit a new application, which requires updated information, repayment of the visa application fee, and another interview by consular officials, unless the interview is waived.[7]

While visas with a longer validity period provide an opportunity for individuals to travel to the United States with greater ease, they do not allow the U.S. Government to receive regularly updated biographic and other information from visitors who travel to the United States multiple times over the validity period of the visas.[8] As such, individuals traveling on visas with longer validity periods are screened using information that is not as recent as for individuals who must obtain visas more frequently.

To alleviate this issue, the U.S. Customs and Border Protection (CBP) developed the Electronic Visa Update System (EVUS). EVUS enables CBP to collect updated information from certain nonimmigrant visa holders[9] prior to travel to the United States without requiring the visa holder to apply for a visa on a more frequent basis.[10] EVUS provides for greater efficiencies in the screening of international travelers by allowing DHS to identify nonimmigrant aliens who may be inadmissible before they depart for the United States, thereby increasing national security and public safety and reducing traveler delays upon arrival at U.S. ports of entry.

In addition to a passport and visa, these designated nonimmigrants are required to enroll in EVUS prior to arrival into the United States. CBP recommends that travelers enroll at least 72 hours prior to boarding an aircraft or vessel carrier destined for the United States, or before applying for admission at a land border port of entry. However, the traveler may enroll any time

---

[6] To determine the validity period of a specific visa category for a given country, a nonimmigrant alien will need to consult the reciprocity schedule for the country that issued their passport, *available at* www.travel.state.gov/content/visas/en/fees/reciprocity-by-country.html.

[7] The visa interview can be waived in certain circumstances, including for renewals that meet specific requirements. *See* INA § 222(h)(1)(B), 8 U.S.C. § 1202(h)(1)(B); 9 FAM 403.5-4(A), *available at* https://fam.state.gov/FAM/09FAM/09FAM040305.html.

[8] The information updates provided through the visa re-application process include basic biographical and eligibility elements that can change over time (e.g., address, name, employment, criminal history).

[9] EVUS enrollment is currently limited to nonimmigrants who hold unrestricted, maximum validity B–1 (business visitor), B–2 (visitor for pleasure), or combination B–1/B–2 visas, which are generally valid for 10 years, contained in a passport issued by the People's Republic of China. Should this list of nonimmigrants be amended, CBP will amend this Privacy Impact Assessment or issue a Privacy Impact Assessment appendix to this Privacy Impact Assessment.

[10] *See* Establishment of the Electronic Visa Update System (EVUS) Final Rule, 81 FR 72481, (Oct. 20, 2016).

prior to boarding an aircraft or vessel destined for the United States, or in the event of land travel, prior to application for admission at a U.S. land border port of entry.

Nonimmigrants enroll in EVUS using an online application that may be completed by either the intended traveler ("applicant") or representative on behalf of the applicant (e.g., friend, relative, or travel industry professional). An applicant or representative may also submit a single enrollment or a group of enrollments at the same time. If this option is selected, the applicant or representative reads and acknowledges the Security Notification/Disclaimer.[11]

Once the disclaimer is acknowledged, an applicant or representative begins the enrollment and is asked to provide certain information, which may include: name; date of birth; phone number; email address; passport information and visa number; information about current or previous employer; destination address and point of contact in the United States; and emergency point of contact information. The user must also answer eligibility questions regarding communicable diseases, arrests and convictions for certain crimes, history of visa revocation or deportation, and other questions. After the applicant or representative completes all required information, the enrollment may be submitted to CBP.

CBP processes the vast majority of EVUS enrollments within minutes; however, CBP may take up to 72 hours to approve or deny an enrollment. Upon receipt, CBP uses this information to vet the EVUS enrollment against selected security and law enforcement databases at DHS, including TECS[12] and ATS,[13] as well as publicly available sources (e.g., social media websites). Once complete, the EVUS website displays the following status messages:

- **Enrolled:** This message indicates a positive determination that the individual's visa is not automatically provisionally revoked and is considered valid for travel to the United States as of the time of the notification.
- **Pending:** The applicant or representative will need to return to the EVUS website later to verify successful enrollment.

[11] This disclaimer notifies the applicant or representative that the information provided in the enrollment will be checked against law enforcement databases. The disclaimer also says EVUS enrollment approval means the applicant is eligible to travel to the United States but does not guarantee admissibility to the United States. Upon arriving at a port of entry, the applicant will be inspected by a CBP Officer who determines admissibility. The applicant or representative must also certify that the information provided must be true and correct and the applicant or representative may be subject to administrative or criminal penalties if they knowingly and willfully provide false, fictitious, or fraudulent information in an EVUS enrollment.

[12] *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.

[13] *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.

- **Unsuccessful:** This message indicates that the submitter may have failed to provide adequate responses to the EVUS questions, attempted to use an invalid passport or visa, such as an expired document or one reported lost or stolen, or irreconcilable errors were discovered relating to the information the applicant or representative provided as part of an attempted EVUS enrollment. An unsuccessful EVUS enrollment will automatically provisionally revoke the individual's visa. An unsuccessful enrollment does not cause the underlying visa to be permanently revoked. An individual who receives an "Unsuccessful Enrollment" message should contact the EVUS Call Center at 00-1-202-325-0180 or via email at evus@cbp.dhs.gov before attempting to re-enroll.
- **The Department of State has revoked your visa:** If this message is displayed, the individual will not be permitted to travel to the United States on that visa. Travel will only be permitted after a new visa application has been submitted, a new visa is issued, and the submitter has successfully enrolled in EVUS based on their new visa.

An "enrolled" EVUS status establishes that the applicant is eligible to travel to the United States, however, it does not guarantee admission to the United States. Upon arrival in the United States, the applicant is still required to undergo inspection by a CBP officer at a port of entry who will determine if the applicant is admissible under U.S. law. An EVUS enrollment is generally valid for multiple trips over a period of two years or until the applicant's passport or visa expires, whichever comes first. This means that as long as the EVUS status remains in "Enrolled" status, the individual does not need to enroll again during the validity period. If the applicant receives an unsuccessful status, it will result in the automatic provisional revocation of the applicant's visa, and the applicant will not be authorized to travel to the United States unless or until they attempt re-enrollment in EVUS and receive and maintain an "Enrolled" status. Once successful, the provisional revocation of the visa will be reversed.

Reason for the PIA Update

CBP is updating this Privacy Impact Assessment to provide notice of changes in the EVUS questionnaire including the optional field to provide social media information.

Optional Collection of Social Media Information

CBP is expanding the EVUS questionnaire to include an optional field in which EVUS applicants may voluntarily provide their current social media identifier(s) or "handle(s)," and social media platform information, though are not required to do so. CBP uses this information for national security and law enforcement vetting purposes and may use tools and search techniques to locate and positively identify social media accounts and profiles belonging to the applicant. CBP

reviews social media information in addition to the DHS system checks described above to further assess an individual's eligibility to travel to the United States.[14]

CBP is responsible for preventing the entry of terrorists and instruments of terrorism into the United States, securing the borders, and enforcing the immigration laws.[15] CBP's authorities empower it to gather information, including information found via social media, which is relevant to its immigration and law enforcement missions.[16] Reviewing an individual's social media presence may identify potential deception, fraud, or previously unidentified national security or law enforcement concerns. Reviewing social media presence may also help CBP distinguish individuals of concern from individuals whose information substantiates their eligibility, as CBP may locate positive, confirmatory information in support of a traveler's eligibility to travel to the United States.

Applicants and representatives who submit EVUS questionnaires on behalf of an applicant have the option to include the social media information as part of the submission. The social media question on the EVUS questionnaire is clearly marked as "optional" and applicants or representatives may submit the EVUS questionnaire without providing such information. A decision to forgo responding to the optional social media question will not result in denial or an "unsuccessful" or "revoked visa" response from EVUS. CBP uses tools and search techniques to locate and positively identify social media accounts and profiles belonging to the applicant. CBP officers use publicly available information,[17] including social media information, as part of the existing EVUS screening and vetting processes irrespective of whether an individual voluntarily provides social media information as part of their EVUS submission.

CBP will use voluntarily provided social media handle(s) and platform(s) to identify correct social media accounts and to vet against selected security and law enforcement databases at DHS, including TECS and ATS. Additionally, CBP National Targeting Center (NTC) analysts may use the social media information supplied on the application to conduct "Overt Research"[18] and "Masked Monitoring" in support of assessing a EVUS application and/or as part of an

[14] In 2018, CBP received approval to collect social media information from EVUS applicants who voluntarily provide their social media information. *See* https://www.federalregister.gov/documents/2017/04/27/2017-08505/agency-information-collection-activities-electronic-visa-update-system.
[15] Homeland Security Act § 402 (6 U.S.C. § 202), and 6 U.S.C. § 211.
[16] 8 U.S.C. §§ 1182, 1187, 1225, 1357(b).
[17] DHS defines publicly available social media information as any electronic social media information that has been published or broadcast for public consumption, is available on request to the public, is accessible online to the public, is available to the public by subscription or purchase, or is otherwise lawfully accessible to the public without establishing a direct relationship (*e.g.,* "friend", "follow", "connect").
[18] "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).

admissibility determination[19] Under no circumstance will DHS/CBP violate any social media privacy settings in the processing of EVUS applications.

CBP retains relevant information from social media platforms collected during the vetting of an EVUS questionnaire in ATS. Although the information collected will largely pertain to user accounts operated by the individual who submitted the EVUS 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 EVUS applicant's "friends," "followers," or "likes"), as well as secondary and tertiary contacts associated with the applicant that pose a potential risk to the United States or demonstrate a nefarious affiliation on the part of the applicant. Relevant information related to each of these contacts may also be retained in ATS and used as part of the vetting process for the EVUS applicant.

As noted above, CBP does not deny EVUS applications solely based on information found on social media. If CBP finds derogatory information within social media, the CBP officer will approve or deny the application based on the totality of the circumstances (e.g., responses to eligibility questions and relevant information found in DHS systems, social media, and other publicly available information).

Privacy Impact Analysis

Authorities and Other Requirements

The collection of the information for EVUS enrollment continues to be authorized by sec. 402(4) of the Homeland Security Act of 2002, 6 U.S.C. § 201, et seq., and sec. 103 (8 U.S.C. § 1103), 214 (8 U.S.C. § 1184), 215 (8 U.S.C. § 1185), and 221 (8 U.S.C. § 1201) of the Immigration and Nationality Act (INA), and 8 CFR part 2.

The DHS/CBP-009 EVUS System of Records Notice (SORN) continues to cover this collection of information.[20] However, CBP is concurrently issuing an update to this System of Records Notice to account for the collection of social media information. While the EVUS System of Records Notice covers the collection of information on the EVUS application, the Automated Targeting System System of Records Notice[21] covers the vetting and storage of vetting results in that system.

---

[19] "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").

[20] *See* DHS/CBP-022 Electronic Visa Update System (EVUS), 84 FR 30751 (June 27, 2019), *available at* https://www.dhs.gov/system-records-notices-sorns.

[21] *See* DHS/CBP-006 Automated Targeting System (ATS), 77 FR 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

Office of Management and Budget (OMB) Control Number 1651-0139 continues to cover the collection of EVUS information under the Paperwork Reduction Act (PRA). OMB approved CBP to add an optional field to the EVUS questionnaire in 2018 for social media information.

Characterization of the Information

With this Privacy Impact Assessment Update, CBP is expanding the EVUS questionnaire to add an optional field to collect social media identifier(s) ("handle(s)") and provider/platform. CBP continues to collect information from the same sources, including individual applicants intending to travel to the United States, as well as representatives who complete the enrollment on behalf of an applicant (e.g., travel agent, family members).

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 EVUS application.

Mitigation: This risk is fully mitigated. There is no requirement for applicants to supply their social media information and therefore, no benefit for an applicant or representative to supply the social media handle of a relative or associate. If an applicant does not have a social media presence, they may indicate so in the questionnaire or leave the field blank. CBP does not consider the lack of social media accounts as derogatory information and a decision to forgo answering the optional question will not result in the denial of an EVUS enrollment. Further, applicants and representatives are required to certify that the information provided in the questionnaire is true and correct. If the applicant or representative knowingly and willfully provides false, fictitious, or fraudulent information, they may be subject to administrative or criminal penalties.

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).

Mitigation: This risk is partially mitigated. The application will specify that the social media field is optional. Further, irrespective of whether the individual provides their social media information, by way of their consent, First Amendment-protected information could be collected when CBP officers use publicly available information, including social media information, as part of the existing EVUS screening and vetting processes pursuant to DHS and CBP's law enforcement mission authorities. While there is a risk of collection of First Amendment-protected activity by CBP, collection that is pertinent to, and within the scope of, an authorized CBP law enforcement activity is permitted under the Privacy Act.[22] DHS policy directs that "DHS personnel shall not collect, maintain in DHS systems, or use information protected by the First Amendment unless (a) an individual has expressly granted their consent for DHS to collect, maintain and use that information; (b) maintaining the record is expressly authorized by a federal statute; or (c) that information is relevant to a criminal, civil, or administrative activity relating to a law DHS enforces

[22] *See* 5 U.S.C. § 552a(e)(7).

or administers."[23] 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 approve or deny an EVUS application, CBP will not collect, maintain, and use such third-party information unless it is necessary and relevant to making a EVUS determination. Further, any such collection must be within the scope of an authorized law enforcement activity, as permitted by subsection (e)(7).

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

Mitigation: This risk is partially mitigated. Information is collected directly from the social media accounts of individuals who are presumed to generally have some degree of control over what is posted on their social media account. CBP, therefore, presumes some of this information is accurate. However, information posted by an associate of the individual on the individual's social media page may also be taken into consideration. Information collected from social media, by itself, will not serve as the sole basis to deny an EVUS application. Instead, CBP uses the totality of information – information submitted as part of the EVUS application along with the information found during CBP vetting, including on social media – to approve or deny the EVUS application. CBP has also developed procedures and training focused on understanding data quality limitations associated with social media.

Privacy Risk: CBP may view and collect information about other individuals who may have posted or interacted with the EVUS applicant on their publicly facing social media platform(s) yet are not EVUS applicants themselves and have no other involvement with DHS or CBP.

Mitigation: This risk is partially mitigated. As described above, CBP will view information about individuals who are associated with an applicant's social media account, and possibly individuals associated with those individuals, even if the individuals do not have a direct connection with CBP. However, CBP will not retain such information unless it is relevant to making an EVUS determination.

Privacy Risk: There is a risk that the applicant or their representative(s) will submit inaccurate information about the EVUS 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 representative

[23] *See* Memorandum from Acting Secretary McAleenan on Information Regarding First Amendment Protected Activities, *available at* https://www.dhs.gov/publication/memo-information-regarding-first-amendment-protected-activities.

submissions. Although CBP cannot prevent applicants or their representatives from submitting inaccurate information, CBP provides opportunities for the applicant or representative to verify the information within the EVUS enrollment prior to submission. If erroneous information is entered, it 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 EVUS vetting process to help inform their questioning of the EVUS enrollee at the port of entry. If an applicant or representative provides information as part of the EVUS enrollment that is later found to be inaccurate, the enrollee may be subject to a secondary inspection upon arrival in the United States. Secondary inspections allow CBP officers to perform a more in-depth interview and conduct additional research without causing delays for other arriving travelers. If referred, a CBP officer will determine admissibility during the secondary inspection. If the individual is found to be inadmissible, their EVUS enrollment may be changed to "unsuccessful," thus provisionally revoking their visa.

Privacy Risk: There is a risk that a representative will not know the social media information related to the EVUS applicant, and, therefore, will leave the field blank or provide inaccurate information.

Mitigation: This risk is partially mitigated. CBP places the onus on the representative to obtain the applicant's correct social media information (if the applicant chooses to provide this information in the optional field). All information provided by the representative must be true and correct. An EVUS enrollment may be revoked at any time and for any reason, including based on new information influencing eligibility. An applicant or representative may be subject to administrative or criminal penalties if false information or fraudulent statements or representation is knowingly and willfully submitted on behalf of the applicant.

Uses of the Information

CBP uses voluntarily provided social media identifiers to conduct screening, vetting, and law enforcement checks of EVUS applicants from publicly available information on social media. CBP also conducts screening, vetting, and law enforcement checks on EVUS applicants using social media irrespective of whether the applicants provide their social media identifiers in EVUS. Use of publicly available information on social media platforms to make an eligibility determination for an EVUS applicant complies with DHS Management Directive (MD) 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 NTC may engage in social media information collection using both "overt research" and "masked monitoring" in support of assessing a EVUS application and/or assessing admissibility. 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 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 n 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 EVUS 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 in support of assessing an EVUS application and/or assessing admissibility. 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 continues to use all information submitted as part of an EVUS application to determine the eligibility of an applicant to travel to the United States and whether the applicant poses a law enforcement or security risk to the United States.[24] CBP also continues to vet the EVUS applicant information against selected security and law enforcement databases at DHS, including TECS and ATS.

CBP retains information from social media platforms collected during the vetting of an EVUS application in ATS. Though the information collected will largely pertain to user accounts operated by the individual that submitted the EVUS application, it is possible that information belonging to the applicant's social media contacts, or the contacts of contacts, will be captured. Through link analysis, CBP may identify direct contacts (such as an EVUS 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. Information related to each of these contacts may be used as part of the vetting process to approve or deny an EVUS application and will be retained in ATS.

[24] *See* 8 U.S.C. § 1187(h)(3).

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

Mitigation: This risk is partially mitigated. CBP analysts are required to respect an individual's privacy settings on social media accounts. CBP analysts will review information on social media platforms in a manner consistent with the privacy settings the social media account holder has chosen to adopt for those platforms. Only that information which the account holder has allowed to be shared publicly will be viewed by CBP. All authorized CBP social media users must sign rules of behavior that explicitly prohibit them from accessing information designated as private on an account. Authorized users must also complete privacy training for the operational use of social media. In order to maintain access as an operational user of social media, CBP users must complete the privacy training and attest to the rules of behavior on an annual basis. Additionally, CBP routinely reviews social media access to remove access from users who no longer require access to social media (e.g., change of job duties or employment). Furthermore, all EVUS application determinations are reviewed by a first line supervisor to verify that the findings are based on all available information (not solely based on information obtained from social media) and assess the completeness and accuracy of the records used to support the determinations. Social media reviews that yield information that could result in the denial of an EVUS application are reviewed by a second line supervisor to ensure that information used in the EVUS determination is accurate, relevant, timely, and complete.

Privacy Risk: There is a risk that CBP will deny an EVUS application if, through vetting, CBP discovers a social media profile that was not disclosed on an EVUS questionnaire.

Mitigation: This risk is mitigated. As noted previously, provision of an individual's social media information is optional. Therefore, while CBP may still vet an individual using information obtained via social media, an individual's EVUS application may not be denied solely because CBP later discovered a social media profile for that individual. However, CBP may use relevant information collected from a social media account to adjudicate a EVUS application. Further, CBP advises applicants and representatives to complete the application fully and honestly; failure to provide accurate and truthful responses to required fields of the EVUS questionnaire may result in denial. CBP uses discretion when reviewing EVUS applications for approval or denial in accordance with the INA.

Notice

CBP is providing notice of these changes through the publication of this Privacy Impact Assessment. Additionally, the EVUS website presents users with a Privacy Act Statement prior to collection of information. The online EVUS application also contains a Frequently Asked

Questions (FAQ) section[25] that addresses the addition of optional social media elements to the EVUS application.

In 2018, CBP also received OMB approval for the optional collection of social media information from EVUS applicants under OMB Number 1651-0139.

Finally, the EVUS System of Records Notice, last published on June 27, 2019, is being updated concurrently with this Privacy Impact Assessment to reflect the optional collection of social media information.

Privacy Risk: There is a risk that friends, family members, associates, or affiliates of the EVUS applicant will not be aware of their inclusion on the EVUS application or their exposure to CBP vetting of the EVUS application. This risk includes associates or affiliates who interact with the EVUS applicant on their social media accounts.

Mitigation: This risk is partially mitigated. As noted previously, whether the applicant chooses to voluntarily provide their social media information in response to the EVUS questionnaire, CBP may conduct vetting of EVUS applicants using social media to include information about the applicant, their contacts, or contacts of contacts. The publication of the updated EVUS System of Records Notice in the Federal Register[26] will provide general notice that optional social media information will be collected. Additionally, the publication of this Privacy Impact Assessment expands the notice regarding the optional social media information collection on the EVUS application and social media vetting by CBP. There is also a FAQ section on the EVUS application that explains to applicants the inclusion of the optional social media information collection. However, individuals who are not the applicant will not receive direct notice of social media collection in the same manner as the EVUS applicant.

Data Retention by the Project

There are no changes to data retention because of this update. CBP continues to retain EVUS application data, including optionally provided social media handle(s), for a maximum of five years in an active database and 10 years in archive status. Additionally, when retaining information collected from social media sources, CBP documents the date, site(s) accessed, information collected, and how it was used, as with any other CBP information collection. CBP may retain social media information in various systems, including ATS, in accordance with the other systems' respective retention schedules. For example, ATS retains information for 15 years.

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

[25] https://www.cbp.gov/travel/international-visitors/electronic-visa-update-system-evus/frequently-asked-questions.

Mitigation: This risk is mitigated. All authorized CBP social media users complete privacy training. Additionally, only information relevant to EVUS eligibility determinations will be retained. CBP will not retain information that is not relevant to an EVUS determination.

Information Sharing

CBP will continue to share EVUS information with federal Intelligence Community partners (e.g., the National Counterterrorism Center), and CBP may share EVUS information on a case-by-case basis with appropriate state, local, tribal, territorial, or international government agencies. There are no new privacy risks related to information sharing.

Redress

This update does not impact how access, redress, and correction may be sought through CBP. If an applicant or representative receives a EVUS denial, they may attempt to enroll again multiple times during the visa validity period. There is no waiting period between enrollment attempts.

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, may participate in the collection of information about EVUS applicants from social media platforms.

Access to the EVUS system for internal CBP users is limited to those personnel with a job-related requirement to access the information. All internal users with access to the system are required to have full background checks. All program managers, IT specialists, analysts, and CBP officers, the latter assuming authorization by the EVUS Security Administrator, will have general access to the system. DHS contractors, specifically those involved with systems support, will also have access to the system.

DHS contractors may have an essential role in designing, developing, implementing, and managing the system due to their specialized expertise. Contractors must complete CBP full field background investigations before they are allowed to access any EVUS data and must receive the same security and privacy training as CBP government employees.

Internal users of EVUS systems and records will be assigned different privileges based on their positions and roles to carry out their official duties. Audits will be conducted to log all privileged user transactions and monitor for abuse. External users, EVUS applicants, or their authorized agents can only create or update their respective “accounts” within the system.

In addition, rules of behavior are established for each major application, including EVUS. These rules of behavior require users to be adequately trained regarding the security of systems to which they are authorized access. These rules also require a periodic assessment of technical,

administrative, and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. Rules of behavior will be posted online prior to login for internal users. In addition, the rules of behavior already in effect for each of the component systems from which EVUS draws will be applied to the program, adding an additional layer of security protection.

Security, including access-related controls, will be certified initially and at specified intervals through the security authorization process for the EVUS system.

Contact Official

Sikina Hasham
Director, Electronic System for Travel Authorization
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 DHS Privacy Office.

_____

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