Privacy Impact Assessment
for the

Electronic Visa Update System (EVUS)

DHS/CBP/PIA-033

August 25, 2016

Contact Point
Suzanne Shepherd
Director - EVUS
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 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 used to collect information from nonimmigrant aliens who 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program and 2) have been issued a U.S. nonimmigrant visa of a designated category. EVUS, similar to the Electronic System for Travel Authorization (ESTA) program, collects updated information in advance of an individual's travel to the United States. EVUS also enables DHS to collect updated information from designated travelers during the interim period between visa applications. CBP is publishing this Privacy Impact Assessment because EVUS is a new system that will collect and use personally identifiable information from individuals who meet the EVUS programmatic criteria, as well as information from U.S. citizens identified on the EVUS enrollment request.

Overview

CBP has a responsibility to balance trade and travel while managing threats to the United States posed by people or cargo entering or exiting the country. By requiring enrollment in EVUS and periodic updates to biographic and other information, CBP is increasing the opportunities to identify individuals who may pose a threat or who are otherwise inadmissible to the United States.

When a nonimmigrant alien applies for a visa to travel to the United States, the visa's validity period can vary considerably depending on which country issued the enrollee's passport. The variation in visa validity periods raises security concerns due to the infrequency in which visa holders may be screened or vetted for threats or inadmissibility. For example, some visas remain valid for up to ten years, without any follow-up or recurrent screening and vetting of visa holders. Although the U.S. Government collects biographic and other pertinent information during the visa application process, there is no mechanism for receiving updated information during the lifespan of a visa. Therefore, in the case of a longer term visa, substantial periods of time may pass without the U.S. Government receiving updated information regarding visa holders, including repeat visitors who travel to the United States multiple times over the life-span of a visa. Implementing EVUS will facilitate greater security as it will allow the United States to receive updated traveler information over the life-span of a visa, instead of only during the visa application process.

EVUS is a web-based system that DHS/CBP developed in 2016 to collect updated information from certain aliens who hold extended-length visas before the alien travels to the

United States. The requirements of EVUS are outlined in the forthcoming EVUS Final Rule,[1] which specifies that nonimmigrant aliens who 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program and 2) have been issued a U.S. nonimmigrant visa of a designated category, must periodically enroll in EVUS. Under EVUS, prior to traveling to the United States, nonimmigrant aliens who 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program and 2) have been issued a U.S. nonimmigrant visa of a designated category seeking to travel to the United States on that visa will be required to enroll in EVUS via an internet-based EVUS enrollment request. All EVUS-identified countries and designated visa categories are listed as an Appendix to this PIA. As more countries and visa categories are added to the EVUS program, this Appendix will be updated.

EVUS enrollees must comply with the following requirements:

- Submit all information requested on the EVUS enrollment;
- Attest that the information submitted is accurate; and
- Pay the subscriber fee.

Enrollees must complete EVUS enrollment before departing for the United States (air and sea travel) or arriving in the United States (land travel). The traveler should 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 prior to boarding an aircraft or vessel carrier 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.

The EVUS enrollment may be completed by an alien directly or by a third party, such as a friend, relative, or travel industry professional (when required). After the enrollment information is submitted, the potential enrollee will receive an electronic status message on the EVUS enrollment website stating "enrolled," "pending," "unsuccessful," or "The State Department has revoked your visa." CBP anticipates that each EVUS enrollment attempt will be adjudicated within 72 hours of submission, although most results will be received shortly after submission. An "enrolled" message indicates that the submission was successful and that the covered alien has a valid notification of compliance.

Enrollment notices are sent via the online EVUS system. There are instances when an enrollment attempt results in an unsuccessful enrollment, such as when the enrollee: 1) fails to provide adequate responses to the EVUS questions; 2) fails to make proper payment of the enrollment fee; 3) attempts to use an invalid passport or visa, such as an expired document; 4) reports lost or stolen passport or visa; 5) irreconcilable errors are discovered relating to the

[1] DHS expects the EVUS Final Rule to publish in the Federal Register in late 2016.

information the enrollee provided as part of an attempted EVUS enrollment. The enrollee will receive notification that the enrollment was unsuccessful and be provided instructions on how to complete a successful enrollment. In the interim, however, the enrollee's visa will be automatically provisionally revoked for failure to comply with EVUS. The automatic visa revocation is not necessarily permanent. An unsuccessful enrollment will be superseded upon successful enrollment. There is no limit on the number of times that a covered alien may reattempt enrollment, subsequent to receiving an "unsuccessful" message.

In certain instances, an EVUS enrollee's visa may be revoked by the Department of State (DOS) for reasons unrelated to EVUS compliance, such as when the visa holder may be ineligible for the visa. In those instances, the visa holder will receive a message stating that "The Department of State has revoked your visa." The visa holder will not be permitted to travel to the United States until a new visa application has been submitted to DOS, been approved, and all EVUS requirements have been met.

EVUS will provide carriers (air travel) with an official determination of an enrollee's eligibility to travel to the United States through the Advance Passenger Information System Quick Query (APIS/AQQ) Program[2] when the carriers initiate an interactive APIS/AQQ query. Visa holders who attempt to enroll but receive an unsuccessful enrollment can make another attempt to enroll of call the CBP call center for further assistance. When a former visa holder's visa has been revoked and he or she receives the message, "The Department of State has revoked your visa," he or she will be directed to the DOS to apply for a new visa, if appropriate. EVUS visa confirmation is a requirement in all ports of entry, not just air. EVUS status will be verified by CBP Officers at land border ports of entry through the EVUS system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

DHS and DOS are establishing EVUS under the authority granted in Immigration and Nationality Act (INA).[3] Section 221(a)(1)(B) of the INA authorizes the State Department to issue nonimmigrant visas to foreign nationals. Section 221(c) of the INA provides that "[a] nonimmigrant visa shall be valid for such periods as shall be by regulations prescribed," and section 221(i) of the INA authorizes the Secretary of State to revoke visas at any time, in his or

[2] *See* https://www.gpo.gov/fdsys/pkg/FR-2015-03-13/html/2015-05798.htm
[3] INA sections 103 (8 U.S.C. §1103), 214 (8 U.S.C. § 1184), 215 (8 U.S.C. § 1185), 221 (8 U.S.C. § 1201), and 8 CFR Part 2.

her discretion. Section 214(a)(1) of the INA specifically authorizes DHS to create conditions for an alien's admission, and Section 215(a)(1) of the INA provides that aliens' entry into the United States may be limited and conditioned by DHS. Section 103 of the INA and 8 CFR 2.1 authorize the Secretary of Homeland Security to administer and enforce the INA and other laws relating to the immigration and naturalization of aliens, and to establish such regulations as he deems necessary for carrying out his authority.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Concurrent with this PIA, CBP is publishing a SORN in the Federal Register to provide notice of the EVUS system and EVUS enrollment.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

EVUS will be added as a subsystem to the e-Business Certification and Accreditation package that received its Authorization to Operate (ATO) renewal on October 7, 2014 and is valid through October 7, 2017. We will submit a Significant Change Request to the CBP Office of Information Technology Security and Technology Policy Branch for review and approval by July 15, 2016. Once approved, the Federal Information Security Management Act (FISMA) ID along with all relevant updates will be documented in the e-Business System Security Plan located in DHS Information Assurance Compliance System.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

EVUS staff is working with the CBP Records Office to establish a NARA record and retention schedule for EVUS. CBP proposes the following schedule that applies to records replicated on the unclassified and classified networks:

Enrollment information submitted to EVUS generally expires and is deemed "inactive" two years after the initial submission of information by the enrollee. In the event that a traveler's passport remains valid for less than two years from the date of successful EVUS enrollment, the EVUS notification of compliance will expire concurrently with the passport. Information in EVUS will be retained for one year after the EVUS notification of compliance expires. After this period, the inactive account information will be purged from online access and archived for 12 years. Data linked at any time during the 15-year retention period (generally 3 years active, 12 years archived), to active law enforcement lookout records, will be matched by CBP to

enforcement activities, investigations, or cases, including EVUS enrollment requests that are unsuccessful or in which the Department of State revoked the visa for reasons unrelated to EVUS, will remain accessible for the life of the law enforcement activities to which they may become related.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Yes. The EVUS program is covered by the PRA, and a new information collection request is pending.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

DHS is developing a fully automated electronic system to collect biographic and other necessary information from certain nonimmigrant aliens with long term visas. By requiring aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category to enroll in EVUS, CBP will be able to collect periodic updates of biographic and other information between longer-length visa periods that would otherwise not be obtained.

As provided in the forthcoming EVUS Final Rule, all aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category will be required to submit, if applicable, the following information EVUS:

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- City and country of birth;
- Gender;
- Email address;
- Telephone number (home, mobile, work, other);

- Home address (address, apartment number, city, state/region);
- Internet protocol (IP) address;
- Visa number
- EVUS enrollment number;
- Global Entry Program Number;
- Country of residence;
- Passport number;
- Passport issuing country;
- Passport issuance date;
- Passport expiration date;
- Department of Treasury Pay.gov payment tracking number (i.e., confirmation of payment; absence of payment confirmation will result in a "not cleared" determination);
- Country of citizenship;
- Other citizenship (country, passport number);
- National identification number, if available;
- Address while visiting the United States (number, street, city, state);
- Emergency point of contact information (name, telephone number, email address);
- U.S. Point of Contact (name, address, telephone number);
- Parents' names;
- Current job title;
- Current or previous employer name;
- Current or previous employer street address; and
- Current or previous employer telephone number.

The categories of records in EVUS also include responses to the following questions:

- Do you have a physical or mental disorder, or are you a drug abuser or addict,[4] or do you currently have any of the following diseases (communicable diseases are specified pursuant to sec. 361(b) of the Public Health Service Act):
    - Cholera
    - Diphtheria
    - Tuberculosis, infection
    - Plague
    - Smallpox
    - Yellow Fever
    - Viral Hemorrhagic Fevers, including Ebola, Lassa, Marburg, Crimean-Congo
    - Severe acute respiratory illnesses capable of transmission to other persons and likely to cause mortality.
- Have you ever been arrested or convicted for a crime that resulted in serious damage to property, or serious harm to another person or government authority?
- Have you ever violated any law related to possessing, using, or distributing illegal drugs?
- Do you seek to engage in or have you ever engaged in terrorist activities, espionage, sabotage, or genocide?
- Have you ever committed fraud or misrepresented yourself or others to obtain, or assist others to obtain, a visa or entry into the United States?
- Are you currently seeking employment in the United States or were you previously employed in the United States without prior permission from the U.S. government?
- Have you ever been denied a U.S. visa you applied for with your current or previous passport, or have you ever been refused admission to the United States or withdrawn your application for admission at a U.S. port of entry? If yes, when and where?
- Have you ever stayed in the United States longer than the admission period granted to you by the U.S. government?

[4]Immigration and Nationality Act 212(a)(1)(A)(iii) and (iv). Pursuant to 8 U.S.C. § 1182(a)(1)(A)(iii) and (iv) aliens may be inadmissible to the United States if they have a physical or mental disorder and behavior associated with the disorder that may pose, or has posed, a threat to the property, safety, or welfare of the alien or others, or to have had a physical or mental disorder and a history of behavior associated with the disorder, which behavior has posed a threat to the property, safety, or welfare of the alien or others and which behavior is likely to recur or to lead to other harmful behavior, or are determined (in accordance with regulations prescribed by the Secretary of Health and Human Services) to be a drug abuser or addict.

- Have you ever been a citizen or national of any other country? If yes, other countries of previous citizenship or nationality?

2.2 What are the sources of the information and how is the information collected for the project?

EVUS will allow aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category to enroll in EVUS via a secure website and will be able to check the status of their enrollment via that same site.

- Enrollees must fill out and submit an online form with the required information.
- The enrollee will review the EVUS requirements and disclaimers prior to completing the online enrolment form.
- The enrollee will provide the required biographic and admissibility data listed above on the electronic form, confirm that the information provided is true and accurate, and submit this information through the EVUS website.
- Once the enrollee has submitted his or her information, he or she will be given a unique tracking number. This tracking number, in combination with some personal data element(s) provided by the enrollee during the enrollment process, can be used by the enrollee to log into the EVUS website to view, update, or change the information he or she submitted, as well as check on the status of his or her EVUS enrollment. An "enrolled" message indicates that the submission was successful and that the enrollee has a valid notification of compliance.
- Significant changes (change of name, passport, visa, date of birth) or updates to the data elements require the enrollee to submit a new EVUS enrollment, because these changes may affect the enrollee's admissibility or reflect a change in the enrollee's ability to travel.
- EVUS enrollment/notification of compliance will be valid for a period of two years from when the notification of compliance is issued or for a shorter period time in situations in which a traveler's passport or visa will expire less than two years from the date of EVUS authorization.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

EVUS does not use commercial sources or publicly available data. However, CBP may use open source and publicly available information to determine EVUS eligibility.

2.4 Discuss how accuracy of the data is ensured.

The individual enrollee or his/her designee submits the information directly to DHS through the online EVUS form. Click-through windows and other advisory notices will be provided on the enrollment request requiring EVUS enrollees to acknowledge, read, and understand the required information and the privacy policy. Enrollees will be further notified that their EVUS will only remain valid so long as the information (other than the travel information related to the particular travel they supplied) is correct and current. The individual or his/her designee is required to certify the information. During the enrollment process, CBP will validate visa authenticity before the system allows submission. After submission, the enrollee's information is checked for accuracy by CBP Officers when the individuals present themselves for inspection at the port of entry. The individual's biographic and passport information will be compared to information submitted on EVUS to verify its accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Given that EVUS requires new enrollment for certain modifications made in EVUS, there is the risk that incorrect information would prevent an enrollee from traveling to the United States using EVUS.

Mitigation: Minor changes such as updating a phone number or address can be made by the enrollee without requiring a new enrollment. Significant changes such as a new passport, name change, or a change in the answers to the eligibility, require reenrollment. This is necessary to protect the identity and information of the enrollee by ensuring that updates are not made to an EVUS enrollment by someone other than the enrollee. By requiring a new enrollment, CBP is mitigating the chances that unwanted and/or inaccurate changes are made by someone other than the enrollee. Individuals who update their EVUS enrollment must do so 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. This risk is mitigated since individuals typically know they have a new passport or name change well in advance of this timing requirement.

Privacy Risk: There is a privacy risk that eligibility determinations about travel will be based on inaccurate information.

Mitigation: This risk is mitigated in several ways. First, direct submission of the information from the source, i.e., EVUS enrollees, or authorized third parties who have permission from the enrollee is presumed to be more accurate. Next, more frequent submissions of information by the enrollee or authorized third party during the visa period also helps ensure that the information remains more current and therefore, more accurate. Further, if the enrollment attempt is unsuccessful because of a deficiency in his/her information (for example, lack of payment, expired passport, etc.), the enrollee has the opportunity to correct the information or resolve the issue. Provisional revocation of the visa will be reversed and the enrollee will be able to travel to the United States as soon as he/she fixes the deficiency and successfully enroll in EVUS. However if travel is denied due to a revoked passport, the traveler will have to contact DOS.

Privacy Risk: There is a risk that an enrollee's EVUS status may change prior to his or her travel.

Mitigation: EVUS status can change at any time. However, this risk is partially mitigated through the notification of individuals via email as soon as their status changes. CBP vets the EVUS enrollment information against selected security and law enforcement databases, including the use of TECS[5] and the Automated Targeting System (ATS).[6] DHS may also vet EVUS enrollment information against security and law enforcement databases at other federal agencies to enhance DHS's ability to determine whether the enrollee poses a security risk to the United States. The results of this vetting may support DHS's initial assessment of whether the enrollee's travel poses a law enforcement or security risk and whether there may be issues which may require separate consideration. The individual must attempt enrollment and receive a notification of compliance prior to boarding a carrier destined to the United States.

The EVUS system will continuously query/vet enrollment information against law enforcement databases. There will be individuals who attempt to travel to the United States and are denied boarding due to a failure to maintain a compliant EVUS due to a change in visa status or updated screening and vetting result.

[5] DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing PIA, December 22, 2010, *available at* www.dhs.gov/privacy.
[6] DHS/CBP/PIA-006 Customs and Border Protection Automated Targeting System (ATS) PIA, August 3, 2007, and subsequent updates, PIA, *available at* www.dhs.gov/privacy.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

DHS, together with DOS, will use the information collected through EVUS to determine if the individual may be inadmissible upon arrival in the United States. Through EVUS, DHS will be able to identify individuals who may require additional consideration through a separate process for visa cancellation or revocation. CBP will use the information entered by the enrollee via the EVUS system to:

1) Forward the information to the mechanized CBP Vetting system[7] (a real-time, instantaneous, copy of the DOS Consular Consolidated Database) to determine whether the individual holds a valid passport issued by an identified country containing a valid visa of a designated category and is eligible for enrollment.

2) Vet the enrollee's data against appropriate systems, such as Terrorist Screening Database (TSDB) biographic records, Interpol lost and stolen passport records, and Department of State's lost and stolen passport records and visa revocations, to determine whether the enrollee may require additional admissibility review through a separate process.

3) Store the enrollment attempt and vetting result (successful enrollment, pending, unsuccessful enrollment, State Department has revoked the visa) within the enrollee's EVUS "account" for subsequent summarization, DHS/CBP management reporting, and limited updates by the enrollee.

4) Return communication to the enrollee of results of the enrollment attempt (successful enrollment, pending, unsuccessful enrollment, DOS has revoked the visa) via the EVUS website.

5) Forward the information to DOS systems in the event that CBP determines that there is information relating to admissibility that separately may counsel in favor of considering the visa for a revocation outside of the EVUS process.

6) Provide EVUS status to APIS/AQQ system for Carriers, for subsequent carrier verification of EVUS status.

7) Verify information on the EVUS enrollment during examination by CBP Officers at Ports of Entry upon arrival.

[7] CBP Vetting is a tool that CBP Officers currently use at the primary inspection locations to determine a real-time status of a traveler's visa. CBP is expanding the use of the CBP Vetting system to include a real-time connection to the EVUS website to enable EVUS enrollees the ability to verify their visa status in real-time. The CBP Vetting tool reduces the incidence of document fraud and provides critical data to CBP Officers who process immigrant and non-immigrant visa recipients at Ports of Entry.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. The EVUS system does not analyze any data in this database for purposes of discovering or locating a predictive pattern or an anomaly. Rather this system reviews name matching and screening using existing DHS IT systems. CBP will examine the enrollment information by screening the enrollee's data through TECS and other appropriate systems such as the Automated Targeting System.

3.3 Are there other components with assigned roles and responsibilities within the system?

Online web access to EVUS will be available to CBP only. However, the information collected by and maintained in EVUS may be shared with all component agencies within DHS on a need to know basis consistent with the component's mission. It will also be provided to designated DOS staff in Consular Affairs. Access to EVUS information within DHS is role-based according to the mission of the component and the user's need to know in performance of his or her official duties.

DHS counterterrorism, law enforcement, and public security communities will be provided with information about suspected or known violators of the law and other persons of concern uncovered via EVUS in a timely manner. CBP may share the EVUS enrollee's PII and screening results with other components within DHS where there is a need to know in accordance with their official responsibilities, including collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders.

3.4 Privacy Impact Analysis: Related to the Uses of Information

EVUS will not determine whether the traveler is, in fact, admissible to the United States, as this function will continue to be performed by a CBP Officer following inspection at a Port of Entry. Having the enrollee fill out the EVUS document online ensures accuracy, because the enrollee is in the best position to supply accurate information and verify its accuracy as it is submitted.

EVUS is a two-tiered system with different types of access for internal DHS or DOS users and external EVUS enrollee users. External users consist of the enrollee and third parties

authorized by the enrollees to enter information on their behalf. Internal users consist of CBP personnel with authorized access to the EVUS system. Authorized DOS users will also be provided read-only access.

External Users

Enrollees can only input information into EVUS through the website, they cannot extract information. When an enrollee logs into EVUS, the enrollment questionnaire is blank, even when the user logs on to make updates to his/her information. This is done so third parties (such as travel agents) are unable to log in and gain access to an enrollee's data through a pre-populated screen. While the nature of the EVUS website permits a third party to enter information into the system on behalf of the enrollee, CBP assumes that the enrollee has consented to the third party's access to his/her personal information.

Privacy Risk: There is a risk of unauthorized third parties gaining access to an enrollee's personal information in EVUS.

Mitigation: Enrollee information is retained in the enrollee's EVUS account and is protected from external users gaining unauthorized access by requiring a unique tracking number in combination with the enrollee's date of birth and passport or visa number. Because the information contained in the passport is not enough to access the EVUS account, someone who has stolen a passport without also obtaining the tracking number will not be able to log in and access the enrollee's PII or check the status of the EVUS enrollment. EVUS enrollees will be advised to keep their passport and tracking number separate. Further, data will be encrypted using the National Institute of Standards and Technology (NIST) approved transport layered security data encryption technology at the interface level to prevent third parties from monitoring or accessing an enrollee's PII when filling out and submitting an EVUS enrollment.

When inaccurate information results in an enrollee being unable to successfully enroll in EVUS, the individual may reattempt enrollment. If the individual receives a message stating "The State Department has revoked your visa", the individual will be directed to a U.S. embassy or consulate to resolve the issue and re-apply for a visa, if appropriate.

Internal Users

Privacy Risk: There is a risk that information will be accessed and misused because DHS employees and contractors have access to enrollee information in the EVUS system.

Mitigation: In order to become an authorized internal user, personnel must successfully complete privacy training and hold a full field background investigation clearance. An internal user must also have a job-related requirement to access the specific information. Additionally, because EVUS will use some aspects of the Advance Passenger Information System (APIS), which resides on the TECS IT platform, all internal users of the EVUS system are required to

complete and pass an annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the system. The TPAAC presents Privacy Act responsibilities and agency policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the internal user's understanding of appropriate controls put in place to protect privacy as they are presented. An internal user must pass the test scenarios to retain access to TECS and more specifically, EVUS. This training is regularly updated.

To further mitigate the risk of misuse of information by DHS employees and contractors with access to EVUS, access to data in EVUS is controlled through passwords and restrictive rules pertaining to user rights. Internal users are limited to roles that define authorized use of the system. Procedural and physical safeguards are utilized such as accountability audits and receipt records. Management oversight is in place to ensure appropriate assignment of roles and access to information.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

CBP provides notice to the individual at the time of the electronic collection on the website via a Privacy Act Notice. If an individual has asked a third party to enter the information, the third party is provided the notice and is required to obtain the consent of the individual before entering the information. In addition, DHS is publishing a Final Rule, a Privacy Act System of Records Notice in the Federal Register, and this PIA describing the new system. EVUS is a new electronic collection of the listed information, and notice will be given to the public through the EVUS SORN in conjunction with this PIA, as well as in real time during an enrollee's use of EVUS. Appropriate notice regarding the data to be collected and the requirement to attest to the accuracy of the data will be included in the information provided via the EVUS website. Outreach for EVUS started in March 2016, and continues to occur through CBP, Mission China, airlines, and travel agents.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

To retain a valid visa for entry into the United States, information must be provided pursuant to applicable statutes. Nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category are subject to the forthcoming EVUS Final Rule. The visa of an individual who declines to provide information necessary to complete an EVUS enrollment will be provisionally revoked until such time as an EVUS enrollment is successfully completed. The only legitimate means of declining to provide the subject information is to choose not to travel the United States.

Individuals do not have the right to consent to particular uses of the information. Individuals may only choose whether or not they will submit their information in order to travel to the United States. Once an individual submits the data for EVUS purposes, he or she cannot exert control over the use of that data, aside from his or her ability to amend specific data elements by accessing his or her account and submitting these data elements.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals will not know that they are required to enroll in EVUS prior to travel.

Mitigation: Adequate notice and disclaimer information, including the consequences of not providing the information requested, is provided to the visa holder and consent is obtained before any information is collected. Permanent writing in addition to an EVUS sticky note will be placed in the passport of nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category. This sticky note will inform travelers of the EVUS requirement.

Individuals required to enroll in EVUS that are unaware of the program will have the opportunity to apply prior to travel. Furthermore, CBP will establish a call center to assist travelers with the system.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

"Notification of compliance" will be issued to individuals upon a successful EVUS enrollment. The notice of compliance is valid for no more than two years. As long as the individual's notification of compliance remains valid, the information must be retained in EVUS. The information is retained to screen prospective travelers who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category for admissibility into the United States. This information is retained for an additional year to permit CBP to extend the expiration date of a notification of compliance with EVUS to a maximum of three years, should it choose to do so. Information will be kept in archives for an additional 12 years to allow retrieval of the information for law enforcement and investigatory purposes. This retention is consistent both with CBP's border search authority and with the border security mission mandated for CBP by Congress.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that information will be kept in EVUS for longer periods than necessary.

Mitigation: This retention is consistent both with CBP's border search authority and with the border security mission mandated for CBP by Congress.

This proposed retention is based upon operational and law enforcement needs. EVUS notifications of compliance are valid for no more than two years. Information is required to be retained in EVUS for as long as the traveler is authorized to travel to the United States. This information is retained for an additional year to permit CBP to extend the expiration date of an EVUS to a maximum of three years, should it choose to do so. Information is kept in archives for an additional 12 years to allow retrieval of the information for law enforcement and investigatory purposes.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information submitted during an EVUS enrollment may be shared under a memorandum of understanding (MOU) with DOS to assist it in determining whether a visa should be revoked or re-issued to the visa holder after and during the EVUS vetting. Carriers also will receive the information regarding the enrollee's EVUS status via the APIS/AQQ system.

Additionally, on a case by case basis information may be shared with appropriate federal, state, local, tribal, and foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order or license, or when DHS believes the information would assist enforcement of civil or criminal laws.

EVUS information may be shared when DHS reasonably believes such use is to assist in anti-terrorism efforts or intelligence gathering related to national or international security or transnational crime. CBP may share information with federal and foreign government intelligence or counterterrorism agencies, or components thereof, in bulk, to assist in counterterrorism or counter-intelligence activities, consistent with an information sharing and access agreement for ongoing, systematic sharing. CBP may also share EVUS information with federal and foreign government intelligence or counterterrorism agencies, or components thereof, in response to queries predicated on a particularized threat to national or international security, or to assist in other intelligence activities.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DHS will share EVUS information with external organizations consistent with the routine uses of the EVUS SORN, which are compatible with the original purpose of collection, "to collect and maintain a record of nonimmigrant aliens holding a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category, and to determine whether there is information that requires separate, additional action." CBP will memorialize these data sharing practices in Memorandum of Understandings (MOU) or Interconnection Security Agreements (ISA), which govern the sharing of EVUS information. Under the terms of these MOUs and ISAs, DOS, other agencies, and the carriers will secure EVUS information consistent with approved security practices that meet DHS standards. Personal information will be kept

secure and confidential[8] and will not be divulged to any person within or outside EVUS program without an official need to know. Sharing with DOS is authorized for purposes of granting or revoking a visa. Recipients from other agencies and carriers will be required by the terms of the information sharing agreement to employ security features to safeguard the shared information.

6.3 Does the project place limitations on re-dissemination?

Yes. Information that is shared with other agencies, federal, state, local, tribal, or foreign, outside of the context of any MOU or other prior written arrangement requires a written request by the agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office, and will only be granted when the request and use are: 1) consistent with the Privacy Act, 2) consistent with published routine uses for EVUS, and 3) with the express written approval of CBP. All three requirements are stated conditions for the receiving agencies to obtain and use the shared information. These conditions are stated in the written authorization provided to the receiving agency and represent the constraints around the use and disclosure of the information at the time of the disclosure.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

MOUs and other written arrangements defining roles and responsibilities will be executed between CBP and each agency that regularly accesses EVUS. The information may be transmitted either electronically or as printed materials to authorized personnel. Electronic communication with other, non-CBP systems, may be enabled via message/query based protocols delivered and received over secure point-to-point network connections between EVUS and the non-CBP system. CBP's external sharing of the data submitted to EVUS complies with statutory requirements for national security and law enforcement systems.

Data sent to air carriers will be transmitted via the secure APIS/AQQ electronic portal, subject to the APIS/AQQ SORN requirements and the ISA requirements with the carriers. Information that is shared with other agencies, federal, state, local, tribal, or foreign, outside of the context of any MOU or other prior written arrangement requires a written request by the agency specifically identifying the type of information sought and purpose for which the information will be used. Authorization to share information in this request scenario is subject to approval by the CBP Privacy and Diversity Office.

[8] The EVUS data is stored electronically at the CBP Data Center in a compartmentalized database safeguarded by passwords, encryption of data at rest by Transparent Data Encryption, and auditing software. Data is secured in full compliance with the requirements of the DHS IT Security Program Handbook.

6.5 Privacy Impact Analysis: Related to Information Sharing.

Privacy Risk: There is a risk that information will be unnecessarily shared with entities outside of CBP.

Mitigation: All external sharing is consistent with the Routine Uses within the published EVUS SORN or with other disclosure provisions of the Privacy Act.[9] When information is shared there is both a written MOU and ISA that is negotiated between CBP and the external requestor. The written arrangements and ISAs are periodically audited and reviewed by CBP and the external requestor's conformance to the use, security, and privacy considerations are verified before Certificates to Operate are issued or renewed.

When sharing information with third parties, the same requirements related to security and privacy that are in place for CBP and DHS apply to the outside entity. Access to CBP data is governed by "need to know" criteria that demand that the receiving entity demonstrate the need for the data before access or interface is granted. This criteria is determined and approved during the information sharing disclosure review process by the CBP Privacy and Diversity Office. Third parties must agree to uphold the same security and privacy measures that are used by CBP and DHS.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Enrollees may access their EVUS information to view and amend their enrollment by providing their EVUS number, birth date, and passport number through the EVUS website. Once they have provided their EVUS number, birth date, and passport number, enrollees may view their EVUS status (successful enrollment, unsuccessful enrollment, pending) and submit limited updates to their travel itinerary information. If an enrollee does not know his or her enrollment number, the individual can provide his or her name, passport number, date of birth, passport issuing country, and visa number to retrieve his or her enrollment number.

Once individuals submit their personal information in EVUS, they will not be able to access it through the EVUS website. Enrollees can see the information they supply on the EVUS website as they fill it out and again before submission, to confirm it is timely and accurate. Enrollees 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, enrollees may update limited information such as point of contacts, U.S. address, emergency

[9] 5 U.S.C. 552a.

point of contact, in their accounts.[10] Corrections to any other data elements will require the enrollee to fill out and submit a new EVUS enrollment request. Enrollees that are not successfully enrolled in EVUS will be directed to reapply. Should the visa holder's visa be revoked by DOS for reasons unrelated to EVUS compliance, the former visa holder should contact a U.S. embassy or consulate to apply for a new visa.

DHS allows persons, including foreign nationals, to seek access under the Privacy Act to obtain information maintained in EVUS. Requests for access to PII contained in EVUS may be submitted to the Customer Service Center at www.cbp.gov (phone: 877-CBP-5511). However, information maintained in EVUS pertaining to the accounting of a sharing with a law enforcement or intelligence entity is exempt from the following provisions of the Privacy Act, pursuant to 5 U.S.C. § 552a(j)(2) or (k)(2). Requests should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. 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.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals have multiple options for correcting inaccurate or erroneous information:

1) Information erroneously submitted by enrollees in EVUS can be corrected by the enrollee via the EVUS web-site by making limited updates to their information or by re-enrolling in EVUS.

2) A CBP Officer may also administratively update the same fields as the enrollee when the enrollee applies for admission to the United States at a port of entry. The CBP Officer will verify documentation presented by the traveler by comparing it against information entered in EVUS and determine whether the enrollment information can be administratively updated. Individuals whose personal information is collected and used by the EVUS program may, to the extent permitted by law, examine their information and request correction of inaccuracies.

3) Individuals who believe EVUS holds inaccurate information about them, or who have questions or concerns relating to personal information and EVUS, can contact the call

[10] Limited updates to basic information such as a phone number or address can be made by the enrollee via his/her account on the EVUS website. Significant changes, such as name, date of birth, passport, or visa information will require the enrollee to create a new EVUS.

center operated by CBP employees and contract staff, that may, in limited circumstances, amend inaccurate information (See 7.1).

4) A person who believes that CBP actions are the result of incorrect or inaccurate information may request information about their records pursuant to procedures provided by the Freedom of Information Act and the access provisions of the Privacy Act of 1974 by writing to:

   U.S. Customs and Border Protection
   Freedom of Information Act Division
   90 K Street NE, 9th Floor
   Washington, D.C. 20229

5) Travelers may also contact the DHS Traveler Redress Inquiry Program (TRIP) at 601 South 12th Street, TSA-901, Arlington, VA, 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible to identify the record(s) at issue.

7.3 How does the project notify individuals about the procedures for correcting their information?

Upon beginning an EVUS enrollment, instructions and an advisory notice are provided notifying the enrollee that they are enrolling in EVUS and that the information provided can be used for admission. Individuals will also be notified through the website and System of Records Notice of the availability of the EVUS Program Privacy Coordinator.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that enrollees cannot seek appeal of the determination through EVUS once the enrollee has submitted information and has been issued a successful or unsuccessful enrollment message.

Mitigation: Individuals are not given access to their information via the EVUS web interface to guard against third parties accessing the enrollee's PII. The enrollee may either correct erroneous information through the measures listed in 7.2 of this PIA, or re-apply for a visa at a U.S. consulate or embassy, where redress will be handled in the form of granting or denying a visa for travel to the United States.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used

in accordance with stated practices in this PIA?

Access to the system for internal 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, in particular those involved with systems support, will also have access to the system.

Contractors to DHS 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 will also 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 enrollees, or their authorized agents, will only have the ability to 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 their systems. 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 by the CBP Security organization through Certification and Accreditation (C&A) of the EVUS system.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All users of the EVUS system are required to complete and pass a bi-annual TECS Privacy Act Awareness Course (TPAAC) to maintain their access to the system. The TPAAC presents Privacy Act responsibilities and CBP policy with regard to the security, sharing, and safeguarding of both official and personally identifiable information. The course also provides a number of sharing and access scenarios to test the user's understanding of appropriate controls

put in place to protect privacy as they are presented. A user must pass the test scenarios to retain access to EVUS. This training is regularly updated.

DHS employees are also required to sign statements acknowledging that they have been trained and understand the security aspects of their systems and comply with the following requirements:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate business purposes and in accordance with applicable laws, regulations, and EVUS policies and procedures.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The personal information collected and maintained by EVUS will be accessed principally by certain employees of DHS components and DOS consular officers. The EVUS program will secure information and the systems on which that information resides by complying with the requirements of the DHS IT Security Program Handbook. This handbook established a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules. In order to gain access to the EVUS information, a user must not only have a need to know, but must also have an appropriate background clearance and completed annual privacy training. A supervisor submits the request to the Office of Information Technology (OIT) at CBP indicating the individual has a need-to-know for official purposes. OIT verifies that the necessary background check and privacy training has been completed prior to issuing a new internal user account. Internal user accounts are reviewed annually to ensure that these standards are maintained. 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.

The MOUs and ISAs with DOS, other agencies, and the carriers specify security and access privileges. The agreements reflect the scope of protection and use of EVUS data by third parties (including other agencies) to follow the same privacy protection guidance as DHS employees.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All MOUs regarding the sharing of EVUS information will be drafted and reviewed by the program manager, component Privacy Officer, and counsel and then sent to DHS for formal review in accordance to the information provided in section 8.0 of this PIA.

Responsible Officials

Suzanne Shepherd, Director, EVUS
Admissibility and Passenger Programs
Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security

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

Approval Signature

Original signed copy on file with DHS Privacy Office.

_____

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

Appendix: EVUS Applicability

EVUS is a web-based system that DHS/CBP developed in 2016 to collect updated information from certain aliens who hold extended-length visas before the alien embarks to the United States. The requirements of EVUS are outlined in the EVUS Final Rule.[11]

Below is a list of approved identified countries and their designated visa categories that must participate in the EVUS program. As the EVUS program expands, this Appendix will be updated.

Identified Country	Designated Visa Category	Final Rule
People's Republic of China (PRC)	All B-1, B-2, and B-1/B-2 non-immigrant tourist visas for business and pleasure issued without restriction for maximum validity, i.e., ten years.	Forthcoming in late 2016.

[11] Document is pending publication.