DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2016-0063]

Privacy Act of 1974; Department of Homeland Security/U.S. Customs and Border Protection (DHS/CBP)-022 Electronic Visa Update System (EVUS) System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "Department of Homeland Security/U.S. Customs and Border Protection – DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records." At the same time, in accordance with 5 U.S.C. sec. 552(j) and (k), DHS proposes to claim certain exemptions for this system. At the same time, in accordance with Privacy Act of 1974, DHS proposes to claim certain exemptions for this system. This system of records will allow the Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP) to collect and maintain records on nonimmigrant aliens who hold a passport that was issued by an identified country approved for inclusion in the EVUS program and have been issued a U.S. nonimmigrant visa of a designated category seeking to travel to the United States. The system of records will also cover records of other persons, including U.S. citizens and lawful permanent residents, whose name is provided to DHS as part of a nonimmigrant alien's EVUS enrollment. Requiring aliens holding passports of identified

countries containing U.S. nonimmigrant visas of a designated category with multiple year validity will allow DHS/CBP to collect updated information. The system is used to ensure a visa holder's information remains current. The information is also used to separately determine whether any admissibility issues may need to be addressed outside the EVUS enrollment process by vetting the information against selected security and law enforcement databases at DHS, including the use of CBP's TECS (not an acronym) (DHS/CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778) and the Automated Targeting System (ATS) (DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297). In addition, ATS retains a copy of EVUS enrollment data to identify EVUS enrollees who may pose a security risk to the United States. The ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems. 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 or, although addressed through a separate process, is admissible to the United States. The results of this vetting may inform DHS's assessment of whether the enrollee's travel poses a law enforcement or security risk and whether the proposed travel should be permitted.

This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: This system will be effective **[INSERT THIRTY DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Comments must be received on or before **[INSERT THIRTY DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0063 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, please visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Debra L. Danisek, (202) 344-1610, Acting CBP Privacy Officer, Privacy and Diversity Office, 1300 Pennsylvania Ave., NW, Washington, D.C. 20229. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, DHS/CBP proposes to establish a new DHS/CBP system of records titled, "DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records."

DHS has developed a fully automated electronic system that enables DHS to collect biographic and other information from certain nonimmigrant aliens on a periodic basis as determined by the Secretary. Specifically, EVUS enables DHS to obtain information from individuals who hold U.S. nonimmigrant visas of a designated category in a passport issued by an identified country. By requiring nonimmigrant 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 biographical and other information over the length of the visa period that would otherwise not be obtained, which may assist in identifying persons who may pose a risk to the United States.

The Electronic Visa Update System is a web-based system developed to collect updated information from visa holders subject to the EVUS program. The EVUS does not change the process for obtaining a visa. However, after issuance of a visa, nonimmigrant aliens subject to the EVUS requirements would need to successfully enroll in EVUS online every two years to ensure their visa remains valid for travel to the United States. The online enrollment will be designed as a user-friendly interface that would allow other persons to assist the traveler in completing the enrollment. Enrollees are able to submit and update biographic information and answer eligibility questions using the EVUS

website. Successful EVUS enrollment is required for nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category. In most cases, the enrollee will obtain an immediate response indicating whether the enrollment is successful. The Electronic Visa Update System enrollment and status must be verified by a carrier prior to the traveler boarding an air or sea carrier. Notifications are sent between DHS/CBP and carriers when the following events occur:

- A traveler books travel
- The Airline/Carrier sends Advance Passenger Information to DHS
- The Airline/Carrier receives one of the following responses:
    - EVUS on file – OK to board carrier
    - No EVUS on file – Check for other valid travel documents
    - EVUS enrollment unsuccessful – Do not allow to travel
    - System Issues – Please resend

Among other functions, CBP vets the EVUS enrollment information against selected security and law enforcement databases, including the use of TECS and the Automated Targeting System (ATS). The ATS will retain a copy of EVUS enrollment data to identify EVUS enrollees who may pose a security risk to the United States. ATS will maintain copies of key elements of certain databases to minimize the impact of processing searches on operational systems and to act as a backup for certain operational systems. 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. Furthermore, the EVUS system will continuously query/vet enrollment information against law enforcement databases. EVUS status can change at any time.

The data elements on the EVUS enrollment questionnaire will make the screening of travelers more robust. The required data elements strengthen security in the EVUS enrollment process by enhancing the capability to identify individuals who may pose a threat to the United States or otherwise be found inadmissible at the time that they apply for entry at a U.S. port of entry. Enrollment in EVUS will not guarantee admission into the United States. CBP will continue to employ standard entry procedures to determine admissibility at U.S. ports of entry.

When a person submits an EVUS enrollment, CBP examines the enrollment questionnaire by screening the enrollee's data through ATS and TECS. The initial and updated biographic information obtained by EVUS is important to identify any concerns regarding future admissibility. Failure to successfully enroll in EVUS when required as described above will result in the automatic provisional revocation of the alien's visa, and the alien will not be authorized to travel to the United States unless or until the alien enrolls in EVUS and obtains a notification of compliance. If a visa is provisionally revoked on the basis of failing to provide or update information to EVUS, the person can

attempt EVUS enrollment again, and if successful the provisional revocation of his/her visa would be reversed. In addition, non-compliance with EVUS would be a basis for commercial carriers to deny boarding to an individual seeking to travel to the United States. Because non-compliance with EVUS results in automatic provisional revocation of the individual's visa, the individual would not have valid travel documents upon attempting to board.

DHS/CBP has authority to operate this system under 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.

Consistent with DHS's information sharing mission, information stored in EVUS may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. Information stored in EVUS may also be shared with other federal security and counterterrorism agencies, as well as on a case-by-case basis to appropriate State, local, tribal, territorial, foreign, or international government agencies. This external sharing takes place after DHS determines that it is compatible with the routine uses set forth in this system of records notice.

Additionally, for ongoing, systematic sharing, DHS completes an information sharing and access agreement with federal partners to establish the terms and conditions of the sharing, including: documenting the need to know, identifying authorized users and uses, protecting the privacy of the data, and ensuring the confidentiality of visa records,

as applicable. This updated system will be included in DHS's inventory of systems of records, located on the DHS website at http://www.dhs.gov/system-records-notices-sorns.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Given the importance of providing privacy protections to international travelers, even prior to the collection of the data elements in EVUS that may include information about U.S. persons, DHS always administratively applies the privacy protections and safeguards of the Privacy Act to all international travelers subject to EVUS. The Electronic Visa Update System falls squarely within the mixed system policy and DHS will continue to extend the administrative protections of the Privacy Act to information about travelers and non-travelers whose information is provided to DHS as part of the EVUS enrollment.

Below is the description of the DHS/CBP-022 Electronic Visa Update System

(EVUS) System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records

Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-022.

System name:

DHS/CBP-022 Electronic Visa Update System (EVUS)

Security classification:

Unclassified. The data may be retained on classified networks but this does not change the nature and character of the data until it is combined with classified information.

System location:

Records are maintained at DHS/CBP Headquarters in Washington, D.C., and in field offices. Records are replicated from the operational system and maintained on the DHS unclassified and classified networks.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

1. Nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category; and
2. Persons, including U.S. Citizens and lawful permanent residents, whose information is provided in response to EVUS enrollment questions.

Categories of records in the system:

Nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category to obtain the required travel authorization by electronically submitting an enrollment consisting of biographic and other data elements via the EVUS website. The categories of records in EVUS include:

- 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;
- 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,[1] 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):

[1] Immigration and Nationality Act 212(a)(1)(A). Pursuant to 8 U.S.C. 1182(a), aliens may be inadmissible to the United States if they have a physical or mental disorder and behavior associated with the disorder

- 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?

---

that may pose, or has posed, a threat to the property, safety, or welfare of the alien or others, or (ii) 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.

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

Authority for maintenance of the system:

Title IV of the Homeland Security Act of 2002, 6.U.S.C. 201 et seq., the Immigration and Naturalization Act, as amended, including sec.s 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; and the Travel Promotion Act of 2009, Pub. L. 111-145, 22 U.S.C. 2131.

Purpose(s):

The purpose of this system is 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.

The Department of Treasury Pay.gov tracking number (associated with the payment information provided to Pay.gov and stored in the Credit/Debit Card Data System, DHS/CBP-003 Credit/Debit Card Data System (CDCDS), 76 FR. 67755 (November 2, 2011)) will be used to process EVUS and third-party administrator fees and to reconcile issues regarding payment between EVUS, CDCDS, and Pay.gov. Payment information will not be used for vetting purposes and is stored in a separate system (CDCDS) from the EVUS enrollment data.

DHS maintains a replica of some or all of the data in EVUS on the unclassified and classified DHS networks to allow for analysis and vetting consistent with the above stated uses, purposes, and this published notice.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the United States Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any Component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To appropriate Federal, State, local, international, tribal, or 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, license, or treaty when DHS determines that the information would assist in the enforcement of civil or criminal laws;

H. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital health interests of a data subject or other persons (e.g., to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk).

I. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure

is appropriate in the proper performance of the official duties of the officer making the disclosure.

J. To a Federal, State, tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection to a program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS Component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

K. To Federal and foreign government intelligence or counterterrorism agencies or components thereof when DHS becomes aware of an indication of a threat or potential threat to national or international security to assist in countering such threat, or to assist in anti-terrorism efforts.

L. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

M. To an organization or individual in either the public or private sector, either foreign or domestic, when there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property.

N. To the carrier transporting an individual to the United States, prior to travel, in response to a request from the carrier, to verify an individual's travel authorization status.

O. To the Department of Treasury's Pay.gov, for payment processing and payment reconciliation purposes.

P. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a subpoena, or in connection with criminal law proceedings.

Q. To appropriate Federal, State, local, international, tribal, or 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, license, or treaty when DHS determines that the information would assist in the enforcement of civil or criminal laws.

R. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

DHS/CBP stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are safeguarded with passwords and encryption and may be stored on magnetic disc, tape, and digital media.

Retrievability:

DHS/CBP may retrieve records by any of the data elements supplied by the enrollee.

Safeguards:

DHS/CBP safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. CBP has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

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 the EVUS notification of compliance, the EVUS enrollment will expire concurrently with the passport. Information in EVUS will be retained for one year after the EVUS travel enrollment expires. After this period, the inactive account information will be purged from online access and archived for 12 years. At any time during the 15-year retention

period (generally 3 years active, 12 years archived) CBP will match data linked to active law enforcement lookout records to enforcement activities, and/or investigations or cases, including EVUS enrollment attempts that are unsuccessful, which will remain accessible for the life of the law enforcement activities to which they may become related. NARA guidelines for retention and archiving of data will apply to EVUS and CBP continues to negotiate with NARA for approval of the EVUS data retention and archiving plan. Records replicated on the unclassified and classified networks will follow the same retention schedule.

Payment information is not stored in EVUS, but is forwarded to Pay.gov and stored in CBP's financial processing system, CDCDS, pursuant to the DHS/CBP-018, CDCDS system of records notice.

When a traveler's EVUS data is used for purposes of processing his or her application for admission to the United States, the EVUS data will be used to create a corresponding admission record in the DHS/CBP-016 Non-Immigrant Information System (NIIS) (March 13, 2015, 80 FR 13398). This corresponding admission record will be retained in accordance with the NIIS retention schedule, which is 75 years.

System Manager and address:

Director, Office of Automated Systems, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue NW, Washington, D.C. 20229.

Notification procedure:

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, he or she can provide his or her name, passport number, date of birth, passport issuing country, and visa number to retrieve his or her enrollment number.

In addition, EVUS enrollees and other individuals whose information is included on EVUS enrollment may submit requests and receive information maintained in this system as it relates to data submitted by or on behalf of a person who travels to the United States and crosses the border, as well as, for EVUS enrollees, the resulting determination (successful enrollment, pending, unsuccessful enrollment). However, the Secretary of Homeland Security has exempted portions of this system from certain provisions of the Privacy Act related to providing the accounting of disclosures to individuals because it is a law enforcement system. CBP will, however, consider individual requests to determine whether or not information may be released. In processing requests for access to information in this system, CBP will review not only the records in the operational system but also the records that were replicated on the unclassified and classified networks, and based on this notice provide appropriate access to the information.

Individuals seeking notification of, and access to, any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters Freedom of Information Act (FOIA) Officer,

whose contact information can be found at http://www.dhs.gov/foia under "FOIA Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive, SW, Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his or her agreement for you to access his or her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See "Notification procedure" above.

Contesting record procedures:

See "Notification procedure" above.

Record source categories:

Records are obtained from the online EVUS enrollment at https://www.cbp.gov/EVUS. Some record information is derived from visa records of the U.S. Department of State.

Exemptions claimed for the system:

No exemption shall be asserted with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who travels to visit the United States and crosses the border, nor shall an exemption be asserted with respect to the resulting determination (authorized to travel, pending, or not authorized to travel). Information in the system may be shared with law enforcement and/or intelligence agencies pursuant to the above routine uses. The Privacy Act requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact

that a law enforcement or intelligence agency has sought and been provided particular records may affect ongoing law enforcement activities. As such, pursuant to 5 U.S.C. 552a(j)(2), DHS will claim exemption from secs (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS will claim exemption from sec. (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information.

Dated: August 29, 2016.

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2016-21100 Filed: 8/31/2016 8:45 am; Publication Date: 9/1/2016]