



9111-14

**DEPARTMENT OF HOMELAND SECURITY**

Docket No. DHS-2018-0046

**Privacy Act of 1974; System of Records: DHS/CBP-022 Electronic Visa Update System (EVUS)**

**AGENCY:** Department of Homeland Security.

**ACTION:** Notice of a Modified System of Records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, “Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-022 Electronic Visa Update System (EVUS) System of Records.”

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

**ADDRESSES:** You may submit comments, identified by docket number DHS-2018-0046 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 DHS-2018-0046. 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, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions, please contact: Debra L. Danisek, (202) 344-1610, [Privacy.CBP@CBP.DHS.GOV](mailto:Privacy.CBP@CBP.DHS.GOV), 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, [Privacy@hq.dhs.gov](mailto:Privacy@hq.dhs.gov), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

**SUPPLEMENTARY INFORMATION:**

I. Background

DHS developed the Electronic Visa Update System (EVUS) as a fully automated web-based 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 a country identified and selected by the Secretary. As part of 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.

EVUS does not change the process for obtaining a visa. After issuance of a visa, nonimmigrant aliens subject to EVUS requirements 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 is designed as a user-friendly interface that would allow other persons to assist the traveler in completing the enrollment. Enrollees submit and update biographic information and answer eligibility questions using the EVUS website. In most cases, the enrollee will obtain a response within seventy-two (72) hours indicating whether the enrollment is successful. The EVUS 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 a travel reservation
- The Airline/Sea Carrier sends Advance Passenger Information to DHS
- The Airline/Sea 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 select security and law enforcement databases, including TECS and the Automated Targeting System (ATS). The ATS retains a copy of EVUS enrollment data to identify EVUS enrollees who may pose a security risk to the United States. 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 that 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 new derogatory information received from law enforcement and other national security databases. An individual's EVUS status can change at any time.

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 nonimmigrant alien's visa, and the nonimmigrant alien will not be authorized to travel to the United States under the provisionally revoked visa unless or until the nonimmigrant 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.

To perform its mission related to the screening of visa holders for potential risks to national security, and due to the constantly evolving threat environment, DHS/CBP is updating this SORN, last published in the *Federal Register* on September 1, 2016, to:

(1) Remove references to specific EVUS application questions and data elements. DHS/CBP is updating the EVUS SORN to clarify that it covers responses to questions about travel history and eligibility for admission to the United States to allow DHS/CBP to evaluate whether a covered alien's travel to the United States poses a law enforcement or security risk. These questions may include eligibility questions regarding, for example: infection with communicable diseases of public health significance, existence of arrests or convictions for certain crimes, past history of visa or admission denial, and previous presence in countries or areas of concern. DHS/CBP will no longer include the specific questions in the EVUS SORN, but will continue to issue updated information collection requests pursuant to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) and 5 CFR 1320.8 seeking public notice and comment, and will amend the EVUS online application, to reflect future changes. Enrollment in EVUS does not guarantee admission into the United States. DHS/CBP will continue to employ standard entry procedures to determine admissibility at U.S. ports of entry.

(2) Update the record source categories for additional transparency about the full vetting process to clarify that all vetting results and other derogatory information collected and maintained by DHS and received by other external partner government agencies are retained in ATS.

(3) Expand the previously issued exemptions to clarify that law enforcement records and other derogatory information in this system derived from CBP's ATS and TECS that is relied upon as a basis for a denial of the EVUS enrollment application may be exempt from certain provisions of the Privacy Act of 1974 because of criminal, civil, and administrative enforcement requirements. Further, other law enforcement records and derogatory information not relied upon in DHS/CBP's EVUS decision is still held in ATS and TECS, and covered by those DHS/CBP SORNs, including any exemptions relied upon by DHS pursuant to those SORNs. DHS/CBP uses information from law enforcement and national security systems to determine whether an EVUS applicant is eligible for travel to the United States. Due to the addition or modification of the exemptions, DHS is issuing a Notice of Proposed Rulemaking concurrent with this system of records notice to exempt this system of records from certain provisions of the Privacy Act of 1974 elsewhere in the *Federal Register*. The previously issued Final Rule to exempt this system of records from certain provisions of the Privacy Act of 1974 (81 FR 85105, November 25, 2016) remains in effect until an updated Final Rule is published.

(4) Add new routine uses and clarifying previously issued routine uses to reflect when EVUS information may be disclosed. First, DHS/CBP is updating Routine Use "E" and adding a new routine use "F" to comply with Office of Management and Budget Memorandum (OMB) M-17-12 pertaining to data breach procedures. Due to the inclusion of a new routine use "F," previously issued routine use "F" has moved to routine use "H." Second, DHS/CBP is

modifying previously issued routine use “G” by adding “or license.” As part of this routine use, while DHS/CBP frequently shares information in connection with specific cases, DHS/CBP also shares data (including in bulk) with another federal agency to proactively identify law enforcement violations consistent with approved information sharing access agreements. Third, DHS/CBP is modifying previously issued “K,” now routine use “M,” to clarify that DHS/CBP may share information either in bulk or on a case-by-case basis to assist other agencies proactively to identify national security and counterterrorism threats for the purposes of intelligence, counterintelligence, or counterterrorism activities authorized by U.S. law, Executive Order (E.O.), or other applicable national security directives. Fourth, DHS/CBP is modifying previously issued routine use “P,” now routine use “R,” to remove disclosures “in response to a subpoena.” Fifth, DHS/CBP is adding routine use “T” to clarify that DHS may share information to agencies lawfully engaged in collecting law enforcement intelligence information in order for them to carry out their law enforcement responsibilities. Sixth, DHS/CBP is adding routine use “V” to provide further transparency of its sharing with the Department of Treasury. Although routine use “G” currently permits DHS/CBP to share with the Department of Treasury’s Office of Foreign Assets Control (OFAC) for law enforcement purposes, DHS/CBP is adding routine use “V” to clarify it is sharing records covered by this SORN with the OFAC in furtherance of its investigation of a violation or enforcing or implementing a statute, rule, regulation, order, or license. OFAC may

then publicly publish information on the List of Specially Designated Nationals and Blocked Persons (SDN List) of individuals and entities whose property and interests in property are blocked or otherwise affected by one or more OFAC economic sanctions programs, as well as information identifying certain property of individuals and entities subject to OFAC economic sanctions programs. For additional information, and procedures for how to access, correct, or amend records on the OFAC SDN list, please see Department of Treasury SORN “DO.120 - Records Related to Office of Foreign Assets Control Economic Sanctions - 81 FR 78298 (Nov. 7, 2016).”

Finally, all prior existing routine uses not mentioned above are currently contained in this revised SORN, but these routine uses may have moved down one or two letters due to the addition of new routine uses. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

The bulk of information stored in this system pertains to nonimmigrant aliens who: 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program by the Secretary, and 2) have been issued a U.S. nonimmigrant visa of a designated category seeking to travel to the United States. Records pertaining to nonimmigrant aliens described in this SORN are not covered by the Privacy Act, and thus, such notice does not confer any legal rights under the Privacy Act to such persons. However, DHS is publishing this SORN to describe all records maintained by DHS/CBP for transparency purposes.

Consistent with DHS’s information sharing mission, information stored in the

DHS/CBP-022 EVUS system of records 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. In addition, DHS/CBP may share information stored in EVUS with appropriate Federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this SORN. 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.

Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This modified system will be included in the Department of Homeland Security's inventory of record systems.

## II. Privacy Act

The Privacy Act of 1974 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 of 1974 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 of 1974, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the

Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act of 1974.

Below is the description of the DHS/CBP-022 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 NAME AND NUMBER:** Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-022 Electronic Visa Update System (EVUS).

**SECURITY CLASSIFICATION:** Unclassified and classified. The unclassified 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.

**SYSTEM MANAGER(S):** Director, EVUS Program Management Office, [evus@cbp.dhs.gov](mailto:evus@cbp.dhs.gov), U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue, NW, Washington, D.C. 20229.

**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 secs. 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 C.F.R. Part

2 and 8 C.F.R. Part 215; and the Travel Promotion Act of 2009, Pub. L. 111-145, 22 U.S.C. sec. 2131.

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to permit DHS/CBP to collect and maintain records on travelers who hold a passport issued by an country identified for inclusion in the EVUS program as selected by the Secretary of Homeland Security, and who have been issued a U.S. nonimmigrant visa of a designated category, in order to determine whether any of those enrollees pose a security risk to the United States over the duration of the visa.

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, covered by DHS/CBP-003 Credit/Debit Card Data System (CDCDS), 76 FR 67755 (Nov. 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 CBP 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.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Categories of individuals covered by this system include:

1. Travelers who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category; and

2. Individuals whose information is provided by the applicant in response to EVUS enrollment questions.

**CATEGORIES OF RECORDS IN THE SYSTEM:** Individuals 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 covered by this EVUS SORN 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:

- History of mental or physical disorders, drug abuse or addiction,<sup>1</sup> and current communicable diseases, fevers, and respiratory illnesses;

---

<sup>1</sup> Immigration and Nationality Act (INA) 212(a)(1)(A). Pursuant to INA 212(a), 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 (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

- Past arrests, criminal convictions, or illegal drug violations;
- Previous engagement in terrorist activities, espionage, sabotage, or genocide;
- History of fraud or misrepresentation;
- Previous unauthorized employment in the United States;
- Past denial of visa, or refusal or withdrawal of application for admission at a U.S. port of entry;
- Previous overstay of authorized admission period in the United States;
- Travel history and information relating to prior travel to or presence in Iraq or Syria, a country designated as a state sponsor of terrorism, or another country or area of concern to determine whether travel to the United States poses a law enforcement or security risk;
- Citizenship and nationality information, with additional detail required for nationals of certain identified countries of concern;

**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. As part of the vetting process, DHS/CBP obtains law enforcement and national security records from appropriate Federal, state, local, international, tribal, or foreign governmental agencies or multilateral governmental organizations to assist DHS in determining EVUS eligibility.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those

---

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.

disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, 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 the U.S. Attorneys Offices, 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, only 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 there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a statute, rule, regulation, order, or license when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. 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 of 1974 requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, that relate to the purpose(s) stated in this SORN, for purposes of testing new technology.

J. 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).

K. 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.

L. 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.

M. To a Federal, state, tribal, local, international, or foreign government agency or entity in order to provide relevant information related to intelligence, counterterrorism, or counterterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directives.

N. 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.

O. 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.

P. 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.

Q. To the Department of Treasury's [Pay.gov](https://www.pay.gov), for payment processing and payment reconciliation purposes.

R. 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, or in connection with criminal law proceedings.

S. To a Federal, state, local agency, tribal, territorial, or other appropriate entity or individual, through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, E.O., or other applicable national security directive.

T. To a Federal, state, local, tribal, territorial, or other foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

U. 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 a clearly unwarranted invasion of personal privacy.

V. To the Department of Treasury's Office of Foreign Assets Control (OFAC) for inclusion on the publicly issued List of Specially Designated Nationals and Blocked Persons (SDN List) of individuals and entities whose property and interests in property are blocked or otherwise affected by one or

more OFAC economic sanctions programs, as well as information identifying certain property of individuals and entities subject to OFAC economic sanctions programs.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** 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.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** DHS/CBP may retrieve records by any of the data elements supplied by the enrollee.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** 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 or 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. 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](https://pay.gov) and stored in CBP's financial processing system, CDCDS, pursuant to the DHS/CBP-018 CDCDS SORN.

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 that is covered in the DHS/CBP-016 Non-Immigrant Information System (NIIS) SORN, 80 FR 13398, March 13, 2015. This corresponding admission record will be retained in accordance with the NIIS retention schedule, which is 75 years.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL 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.

**RECORD ACCESS PROCEDURES:** 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 of 1974 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 of 1974 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 an individual seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform to the Privacy Act of 1974 regulations set forth in 6 CFR part 5. The individual must first verify his/her identity, meaning that the individual must provide his or her full name, current address, and date and place of birth. The individual must sign his/her request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual 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, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual 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 an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from that individual certifying his or her agreement for the first individual to access to his/ her records.

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

**CONTESTING RECORD PROCEDURES:** For records covered by the Privacy Act of 1974 or covered JRA records, see "Record Access Procedures" above. For records not covered by the Privacy Act of 1974 or JRA, individuals may submit an inquiry to the DHS Traveler Redress Inquiry Program (DHS TRIP) at <https://www.dhs.gov/dhs-trip> or the CBP INFO CENTER at [www.help.cbp.gov](http://www.help.cbp.gov) or (877) 227-5511 (international callers may use (202) 325-8000 and TTY users may dial (866) 880-6582).

**NOTIFICATION PROCEDURES:** See "Record Access Procedure."

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:**

Pursuant to 6 CFR Part 5, Appendix C, law enforcement and other derogatory information covered in this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, pursuant to 5 U.S.C. 552a (k)(1) and (k)(2): 5 U.S.C. 552a(c)(3); (d)(1), (d)(2), (d)(3), and (d)(4); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

Despite the exemptions taken on this system of records, DHS/CBP is not taking any exemption from subsection (d) 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). However, pursuant to 5 U.S.C. 552a(j)(2), DHS/CBP plans to exempt such information in this system from sections (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. CBP will not disclose the fact that a law enforcement or intelligence agency has sought particular records because it may affect ongoing law enforcement activities.

When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j) or (k), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. For instance, as part of the vetting process, this system may incorporate records from CBP's ATS, and all of the exemptions for CBP's ATS SORN, described and referenced herein, carry forward and will be claimed by DHS/CBP.

**HISTORY:**

DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records, 81 FR 60371 (September 1, 2016).

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

[FR Doc. 2019-13641 Filed: 6/26/2019 8:45 am; Publication Date: 6/27/2019]