DEPARTMENT OF HOMELAND SECURITY

Docket No. DHS-2018-0044

Privacy Act of 1974; System of Records DHS/CBP-009 Electronic System for Travel Authorization (ESTA)

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)-009 Electronic System for Travel Authorization (ESTA) System of Records." This system of records notice (SORN) describes DHS/CBP's collection and maintenance of records that pertain to eligible international travelers who wish to travel to the United States under the Visa Waiver Program (VWP) and have applied for an ESTA travel authorization and persons whose information is provided in response to an ESTA application or Form I-94W questions.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication, and modified and new routine uses and exemptions will become effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2018-0044 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-2018-0044. 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, CBP Privacy Officer, Privacy and Diversity Office, 1300 Pennsylvania Ave., N.W., Washington, D.C. 20229. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Privacy@hq.dhs.gov, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In 2007, Congress enacted the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53. Section 711 of that Act sought to address the security vulnerabilities associated with VWP travelers not being subject to the same degree of screening as other international visitors. As a result, section 711 required DHS to develop and implement a fully automated electronic travel authorization system to

collect biographic and other information necessary to evaluate the security risks and eligibility of an applicant to travel to the United States under the VWP. The VWP is a travel facilitation program that has evolved to include more robust security standards that are designed to prevent terrorists and other criminal actors from exploiting the program to enter the country.

DHS/CBP developed ESTA, a web-based system, in 2008 to determine the eligibility of international travelers to travel to the United States under the VWP. Using the ESTA website, applicants submit biographic information and answer questions that permit DHS/CBP to determine eligibility for travel under the VWP. DHS/CBP uses the information submitted to ESTA to make a determination regarding whether the applicant is eligible to travel under the VWP, including whether his or her intended travel poses a law enforcement or security risk. DHS/CBP vets the ESTA applicant information against selected security and law enforcement databases, including TECS (DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008)) and ATS (DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012)). The ATS also retains a copy of the ESTA application data to vet ESTA applicants against DHS/CBP holdings to determine whether the applicant poses a security risk to the United States. DHS may also vet ESTA application information against security and law enforcement databases owned and operated at other federal agencies to enhance DHS's ability to determine whether the applicant poses a security risk to the United States or is otherwise eligible to travel to and enter the United States under the VWP.

The results of this vetting may inform DHS's assessment of whether the applicant's travel poses a law enforcement or security risk. The ESTA eligibility

determination is made prior to an alien arriving for inspection in the United States. All ESTA vetting results, and derogatory information, are stored in ATS, and covered by the ATS SORN.

To perform its mission related to the screening of international travelers from VWP countries, including alien visitors, for potential risks to national security and the determination of admissibility to the United States, and due to the constantly evolving threat environment, DHS/CBP is updating this SORN, last published September 2, 2016, to:

(1) Expand the category of individuals to clarify that travelers entering the United States under the VWP may do so via air, land, and sea ports of entry. The previously issued SORN referred specifically to VWP travelers entering the United States via air and sea; however, VWP travelers may also transit through land ports of entry.

(2) Clarify that this system of records covers records obtained on the Form I-94W "Nonimmigrant Visa Waiver Arrival/Departure Record," the paper version of ESTA. The Form I-94W is functionally the same as the ESTA, however it is completed at a land port of entry if an individual has not submitted an ESTA application. This is not a new form and has been in use since prior to the launch of the ESTA program.

(3) Clarify that the ESTA application includes questions about travel to any Department of State-designated state sponsor of terrorism, and that DHS/CBP will no longer list the specific countries in this SORN. Section 217(a)(12)(A)(i), of the Immigration and Nationality Act, 8 U.S.C. 1187(a)(12)(A)(i) bars from travel under the VWP nationals of VWP program countries who have "been present, at any time on or after March 1, 2011,"… "in a country that is designated by the Secretary of State" as a

state sponsor of terrorism. If countries are added or removed from the Department of State designation, DHS/CBP will issue an updated information collection request pursuant to the Paperwork Reduction Act of 1995 (44 U.S.C. §3501 *et seq.*) and 5 C.F.R. § 1320.8 seeking public notice and comment, and will amend the ESTA online application.

(4) Specify that vetting results are retained in ATS to provide additional transparency about the full vetting process, and to clarify that any derogatory information obtained from a partner government agency is also stored in ATS. As part of the vetting process, DHS/CBP obtains records from appropriate Federal, state, local, international, tribal, or foreign governmental agencies or multilateral governmental organizations to assist DHS in determining ESTA eligibility.

(5) Clarify or expand previously issued routine uses, and add new routine uses. First, DHS/CBP is modifying existing routine use "E" and adding routine use "F" to be in conformity with Office of Management and Budget (OMB) Memorandum 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 the existing and still remaining routine use "G," by adding "or license." Third, DHS/CBP is adding a new routine use "J" that would permit disclosure to outside 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 relates to the purpose(s) stated in this SORN, for purposes of testing new technology. Fourth, DHS/CBP is expanding the new routine use "M" – previously routine use "K" – to clarify that DHS/CBP may share information to assist agencies proactively identify national

security and counterterrorism threats. Fifth, DHS/CBP is modifying routine use "R," previously routine use "P," to remove disclosures "in response to a subpoena." Sixth, DHS/CBP is adding routine use "S" 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 "S" to clarify it is sharing records covered by this SORN with 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.

(6) Expand the previously issued exemptions to clarify that law enforcement records and other derogatory information derived from DHS/CBP's ATS may be exempt from certain provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. DHS/CBP uses information from law enforcement and

national security systems to determine whether an ESTA applicant is eligible for travel to the United States.

(7) Remove references to the specific ESTA application questions and data elements (which are publicly available on the ESTA website and OMB Number 1651-0111 "Arrival and Departure Record, Nonimmigrant Visa Waiver Arrival/Departure, Electronic System for Travel Authorization (ESTA)") and instead include them as broad categories of questions that are included on the application.

DHS/CBP is issuing a Notice of Proposed Rulemaking for these expanded exemptions concurrent with this Notice. The previously issued Final Rule to exempt this system of records from certain provisions of the Privacy Act (74 FR 45070 (August 31, 2009)) remains in effect until an updated Final Rule is published.

The bulk of information stored in this system pertains to eligible international travelers who wish to travel to the United States under the VWP and have applied for an ESTA travel authorization and persons whose information is provided in response to ESTA application or Form I-94W questions. Most international travelers under the VWP are nonimmigrant aliens, and thus are not "individuals" as defined by the Privacy Act. Accordingly, this 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 and to assist those with rights under the Judicial Redress Act better understand the nature of the records.

Consistent with DHS's information sharing mission, information stored in the "DHS/CBP-009 Electronic System for Travel Authorization 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 ESTA in bulk as well as well as on a case-by-case basis with appropriate Federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this SORN. DHS/CBP documents ongoing, systematic sharing with partners, including documenting the need to know, authorized users and uses, and the privacy protections that will be applied to the data.

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. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right 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.

Below is the description of the DHS/U.S. Customs and Border Protection-009 Electronic System for Travel Authorization System of Records.

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

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization System (ESTA).

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

SYSTEM MANAGER(S): Director, ESTA Program Management Office, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., 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 8 U.S.C. 1187(a)(11) and (h)(3), and implementing regulations contained in 8 C.F.R. part 217; the Travel Promotion Act of 2009, Pub. L. 111-145, 22 U.S.C. 2131.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect and maintain a record of applicants who want to travel to the United States under the VWP, and to determine whether applicants are eligible to travel to and enter the United States under the VWP. The information provided through ESTA is also vetted—along with other information that the Secretary of Homeland Security determines is necessary, including

information about other persons included on the ESTA application—against various security and law enforcement databases to identify those applicants who pose a security risk to the United States and to inform CBP's decision to approve or deny the applicant's ESTA application. This vetting includes consideration of the applicant's IP address, social media information, and all information provided in response to the ESTA application questionnaire, including all free text write-in responses.

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 ESTA and third-party administrator fees and to reconcile issues regarding payment between ESTA, CDCDS, and Pay.gov. Payment information will not be used for vetting purposes and is stored in a separate system (CDCDS) from the ESTA application data.

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include eligible travelers who wish to travel to the United States under the VWP and have applied for an ESTA travel authorization and individuals whose information is provided in response to ESTA application or Form I-94W questions.

CATEGORIES OF RECORDS IN THE SYSTEM:

Visa Waiver Program travelers may seek the required travel authorization by electronically submitting an application consisting of biographical and other data elements via the ESTA website. The categories of records in ESTA include:

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- Country of birth;
- Gender;
- Email address;
- Visa numbers, Laissez-Passer numbers, or Identity card numbers;
- Social media identifiers, such as username(s) and platforms used;
- Publicly available information from social media websites or platforms;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, state/region);
- Internet protocol (IP) address;
- ESTA application number;
- Global Entry Program Number;
- Country of residence;
- Passport information;
- Department of Treasury Pay.gov payment tracking number information;
- Countries of citizenship and nationality;
- National identification number, if available;

- Address while visiting the United States;
- Emergency point of contact information;
- U.S. Point of Contact information;
- Parents' names; and
- Current and previous employer information.

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

- History of mental or physical disorders, drug abuse or addiction,[1] and current communicable diseases, fevers, and respiratory illnesses;
- 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;[2] and

[1] 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 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.

- Citizenship and nationality information, with additional detail required for nationals of certain identified countries of concern.

RECORD SOURCE CATEGORIES: DHS/CBP obtains records from information submitted by travelers either via the (1) online ESTA application form available at https://esta.cbp.dhs.gov/esta/ or (2) the Form I-94W, the paper equivalent to the ESTA portion related to travel authorization, which is used primarily at the land border by VWP travelers or on specific occasions at other ports of entry, without immediate access to the electronic format above. DHS/CBP may also use information obtained from publicly available sources, including social media, to determine ESTA eligibility. 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 ESTA eligibility.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under the Privacy Act, 5 U.S.C. 552a(b), 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 agencies 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] INA 212(a)(12); 8 U.S.C. 1187(a)(12).

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 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 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).

J. 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.

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 or 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, counterintelligence, or counterterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

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, 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 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.

T. 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.

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 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 applicant.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Application information submitted to ESTA generally expires and is deemed "inactive" two years after the initial submission of information by the applicant. In the event that a traveler's passport remains valid for less than two years from the date of the ESTA approval, the ESTA travel authorization will expire concurrently with the passport. Information in ESTA will be retained for one year after the ESTA travel authorization 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 DHS/CBP to enforcement activities, and/or investigations or cases, including ESTA applications that are denied authorization to travel, 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 ESTA, but is forwarded to Pay.gov and stored in DHS/CBP's financial processing system, CDCDS,

pursuant to the DHS/CBP-018, CDCDS SORN. When a VWP traveler's ESTA data is used for purposes of processing his or her application for admission to the United States, the ESTA data will be used to create a corresponding admission record in the DHS/CBP-016 Non-Immigrant Information System (NIIS). 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. DHS/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: Applicants may access their ESTA information to view and amend their applications by providing their ESTA number, birth date, and passport number. Once they have provided their ESTA number, birth date, and passport number, applicants may view their ESTA status (authorized to travel, not authorized to travel, pending) and submit limited updates to their travel itinerary information. If an applicant does not know his or her application number, he or she can provide his or her name, passport number, date of birth, and passport issuing country to retrieve his or her application number.

In addition, ESTA applicants and other individuals whose information is included on ESTA applications 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 ESTA applicants, the resulting determination (authorized to travel, pending, or not authorized to travel). 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. DHS/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, DHS/CBP will review the records in the operational system and coordinate with DHS to ensure that records that were replicated on the unclassified and classified networks, are reviewed and based on this notice provide appropriate access to the information.

Individuals seeking access to and notification of 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 FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts 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, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must

first verify his/her identity, meaning that the individual must provide his/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/her agreement for the first individual to access 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 or covered JRA records, see "Record Access Procedures" above.

NOTIFICATION PROCEDURES: See "Record Access Procedures."

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 6 CFR Part 5, Appendix C, 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. As such, 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).

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 section (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.

HISTORY:

DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 81 FR 60713 (September 2, 2016); DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 81 FR 39680 (June 17, 2016); DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 81 FR 8979 (February 23, 2016); DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 79 FR 65414 (November 4, 2014); DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 77 FR 44642 (July 30, 2012); DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 76 FR 67751 (November 2, 2011); DHS/CBP-009 Electronic System for Travel Authorization (ESTA), 73 FR 32720 (June 10, 2008).

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2019-13645 Filed: 6/26/2019 8:45 am; Publication Date: 6/27/2019]