DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2016-0054]

Privacy Act of 1974; Department of Homeland Security, U.S. Customs and Border Protection-009 Electronic System for Travel Authorization 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 update and reissue the DHS system of records titled, "DHS/U.S. Customs and Border Protection (CBP)-009 Electronic System for Travel Authorization (ESTA) System of Records." This system of records allows DHS/CBP to collect and maintain records on nonimmigrant aliens seeking to travel to the United States under the Visa Waiver Program and other persons, including U.S. citizens and lawful permanent residents, whose names are provided to DHS as part of a nonimmigrant alien's ESTA application or Form I-94W. The system is used to determine whether an applicant is eligible to travel to and enter the United States under the Visa Waiver Program (VWP) by vetting his or her ESTA application information or Form I-94W information against selected security and law enforcement databases at DHS, including TECS (not an acronym) and the Automated Targeting System (ATS). In addition, ATS retains a copy of ESTA application and Form I-94W data to identify individuals from Visa Waiver Program countries 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 ESTA application information against security and law enforcement databases at other federal agencies to enhance DHS's ability to determine whether the applicant poses a security risk to the United States and is 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 and whether the application should be approved.

DHS/CBP is updating this system of records notice, last published on June 17, 2016, to clarify the category of individuals, expand a routine use, and expand the record source categories to include information collected from publicly available sources, such as social media.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This updated system will be effective **[insert date 30 days after DATE OF publication in the FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0054 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 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., N.W., 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. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is updating and reissuing a current DHS system of records titled, "DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records."

In the wake of September 11, 2001, Congress enacted the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53. Section 711 of that Act sought to address the security vulnerabilities associated with Visa Waiver Program (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 biographical 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.

Electronic System for Travel Authorization is a web-based system that DHS/CBP developed in 2008 to determine the eligibility of foreign nationals to travel by air or sea to the United States under the VWP. Using the ESTA website, applicants submit biographic information and answer questions that permit DHS 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. If eligible individuals from VWP countries attempt to enter the United States without an ESTA, they must file a Form I-94W at the time of entry. DHS/CBP vets the ESTA applicant information and Form I-94W 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 and Form I-94W data to identify individuals 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 ESTA and Form I-94W application information against security and law enforcement databases 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 a visitor boarding a carrier *en route* to the United States.

Due to the ongoing national security concerns surrounding foreign fighters exploiting the VWP, DHS/CBP is updating this system of records notice, last published on June 17, 2016 (81 FR 39680), to give notice of a clarification to the category of individuals to include individuals who are eligible for an ESTA but instead submit a Form I-94W (likely during a land border crossing) and an expanded category of records to include responses to a voluntary question requesting ESTA applicants provide their social media identifiers (such as username), to assist DHS/CBP in determining eligibility to travel under the VWP. DHS/CBP is also modifying the overall description of when information may be shared as a routine use pursuant to 5 U.S.C. 552a(b)(3), and expanding Routine Use G to include additional DHS/CBP requirements for information sharing. Lastly, DHS/CBP is also expanding the record source categories to include information collected from publicly available sources, such as social media.

On June 23, 2016 DHS/CBP published in the Federal Register a notice of a proposed revision to ESTA and the I-94W under the Paperwork Reduction Act to add an

optional data field to request social media identifiers (see 81 FR 40892). The 60-day public comment period on the proposed revision to ESTA and the I-94W closed on August 22, 2016. Individuals who submitted comments during the 60-day public comment period can find DHS/CBP response on www.reginfo.gov (Reference OMB Control Number 1651-0111). On August 31, 2016, DHS will publish a notice in the Federal Register that will give the public an additional 30 days to submit comments on the proposed revision to the ESTA and I-94W.

DHS is publishing this revised system of records notice to include, among other things, the social media identifiers included in the proposed revision to ESTA and the I-94W. While this SORN will allow DHS to maintain the information described herein, DHS will not be able to collect social media identifiers using ESTA and I-94W until OMB approves the DHS/CBP's Information Collection Request under the Paperwork Reduction Act (OMB Control Number 1651-0111).

Adding social media data will enhance the existing process, and provide DHS/CBP greater clarity and visibility to possible nefarious activity and connections by providing an additional tool set which DHS/CBP may use to make better informed eligibility determinations. DHS/CBP's collection of a subject's social media identifiers adds another layer of information to the analysis for eligibility determination by providing potential further leads to terrorism or criminal activity.

DHS/CBP is modifying the overall description of when information may be shared as a routine use pursuant to 5 U.S.C. 552a(b)(3), to clarify that information covered by this system of records notice may be shared either in bulk, or on a case-by-

case basis. DHS/CBP is expanding Routine Use G to clarify that DHS may share information when it determines that the information would assist in the enforcement of civil or criminal matters, and not only when the record itself facially indicates a violation or potential violation of law. DHS/CBP is frequently called upon to share information in connection with specific cases, DHS/CBP also shares data (including in bulk) that may be used by another agency to vet against the other agency's databases to identify violations proactively. The updated Routine Use G also clarifies that DHS/CBP is able to share information, consistent with its many international arrangements, relating to the enforcement of licenses or treaties.

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 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 system of records notice. 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.

DHS/CBP previously issued a Final Rule to exempt this system of records from certain provisions of the Privacy Act on August 31, 2009 (74 FR 45069). These regulations remain in effect. This updated system will be included in DHS's inventory of

record systems.

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, and because the ESTA application has generally solicited contact information about U.S. persons, DHS always administratively applied the privacy protections and safeguards of the Privacy Act to all international travelers subject to ESTA. The ESTA falls 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 ESTA application.

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

System name:

DHS/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:

DHS/CBP maintains records 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.

Categories of individuals covered by the system:

Categories of individuals covered by this system include:

1. Persons who seek to enter the United States under the VWP; and,
2. Persons, including U.S. Citizens and lawful permanent residents, 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;
- City of birth;
- Country of birth;
- Gender;
- Email address;
- 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 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 ESTA 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

[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.

specified pursuant to sec. 361(b) of the Public Health Service Act):

  - Cholera
  - Diphtheria
  - Tuberculosis, infection
  - Plague
  - Smallpox
  - Yellow Fever
  - Viral Hemorrhagic Fevers, including Ebola, Lassa, Marburg, Crimean-Congo
  - Severe acute respiratory illnesses capable of transmission to other persons and likely to cause mortality.

- Have you ever been arrested or convicted for a crime that resulted in serious damage to property, or serious harm to another person or government authority?
- Have you ever violated any law related to possessing, using, or distributing illegal drugs?
- Do you seek to engage in or have you ever engaged in terrorist activities, espionage, sabotage, or genocide?
- Have you ever committed fraud or misrepresented yourself or others to obtain, or assist others to obtain, a visa or entry into the United States?
- Are you currently seeking employment in the United States or were you previously employed in the United States without prior permission from the U.S. Government?

- Have you ever been denied a U.S. visa you applied for with your current or previous passport, or have you ever been refused admission to the United States or withdrawn your application for admission at a U.S. port of entry? If yes, when and where?
- Have you ever stayed in the United States longer than the admission period granted to you by the U.S. Government?
- Have you traveled to, or been present in, Iraq, Syria, Iran, Sudan, Somalia, Libya, or Yemen on or after March 1, 2011? If yes, provide the country, date(s) of travel, and reason for travel. Depending on the purpose of travel to these countries, additional responses may be required including:
    - Previous countries of travel;
    - Dates of previous travel;
    - Countries of previous citizenship;
    - Other current or previous passports;
    - Visa numbers;
    - Laissez-Passer numbers;
    - Identity card numbers;
    - Organization, company, or entity on behalf of which you traveled;
    - Official position/title with the organization, company, or entity behalf of which you traveled;
    - Contact information for organization, company, or entity on behalf of which you traveled;

- Iraqi, Syrian, Iranian, Sudanese, Somali, Libyan, or Yemeni Visa Number;
- I-Visa, G-Visa, or A-Visa number, if issued by a U.S. Embassy or Consulate;
- All organizations, companies, or entities with which you had business dealings, or humanitarian contact;
- Grant number, if applicant's organization has received U.S. Government funding for humanitarian assistance within the last five years;
- Additional passport information (if issued a passport or national identity card for travel by any other country), including country, expiration year, and passport or identification card number;
- Any other information provided voluntarily in open, write-in fields provided to the ESTA applicant.

- Have you ever been a citizen or national of any other country? If yes, other countries of previous citizenship or nationality? If Iraq, Syria, Iran, Sudan, Somalia, Libya, or Yemen are selected, follow-up questions are asked regarding status of current citizenship including dual-citizenship information, and how citizenship was acquired.

Applicants who identify Iraq, Syria, Iran, Sudan, Somalia, Libya, or Yemen as their Country of Birth on ESTA will be directed to follow-up questions to determine whether they currently are a national or dual national of their country of birth.

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 part 217, title 8, Code of Federal Regulations; the Travel Promotion Act of 2009, Pub. L. No. 111-145, 22 U.S.C. 2131.

Purpose(s):

The purpose of this system is to collect and maintain a record of persons 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. 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.

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 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 law, rule, regulation, or order, 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 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 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.

K. To federal and foreign government intelligence or counterterrorism agencies or components 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 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 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 applicant.

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.

Retention and disposal:

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. NARA guidelines for retention and archiving of data will apply to ESTA and DHS/CBP continues to negotiate with NARA for approval of the ESTA 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 ESTA, but is forwarded to Pay.gov and stored in DHS/CBP's financial processing system, CDCDS, pursuant to the DHS/CBP-018, CDCDS system of records notice. 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.

System Manager and address:

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

Notification procedure:

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 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 S.W., 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 FOIA Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, individuals 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:

DHS/CBP obtains records from information submitted by travelers via the online ESTA application at https://esta.cbp.dhs.gov/esta/. DHS/CBP may also use information

obtained from publicly available sources, including social media, to determine ESTA eligibility.

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 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.

Dated: August 30, 2016.

Jonathan R. Cantor,

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2016-21210 Filed: 8/31/2016 4:15 pm; Publication Date: 9/2/2016]