9110-06

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0045]

Privacy Act of 1974; Department of Homeland Security U.S. Customs and Border Protection- DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records

AGENCY: Privacy Office, Department of Homeland Security.

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 a current DHS system of records titled, "Department of Homeland Security/U.S. Customs and Border Protection-DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records." This system collects and maintains a record of nonimmigrant aliens seeking to travel to the United States under the Visa Waiver Program. The system is used to determine whether the applicant is eligible to travel to the United States under the Visa Waiver Program by vetting the application information against selected security and law enforcement databases using U.S. Customs and Border Protection (CBP) TECS and the Automated Targeting System (ATS). In addition, ATS retains a copy of ESTA application data to identify potential high-risk ESTA applicants. DHS/CBP is updating this system of records notice to clarify the categories of individuals and remove unnecessary language,

add the Internet Protocol address associated with the submitted ESTA application as a category of records, provide more specific legal authorities, clarify the purposes to include the identification of high-risk applicants, include an additional routine use for judicial proceedings and update and clarify other routine uses, clarify the retention of records in ESTA and the Nonimmigrant Information System (DHS/CBP-016 - Nonimmigrant Information System December 19, 2008 73 Fed. Reg. 77739), update the notification procedures to explain the extension of access procedures to international travelers, allow limited direct access and amendment of ESTA application data, and add the CPB access request address; eliminate unnecessary language from the record source categories, and clarify which exemptions will be used for which provisions of the Privacy Act. The Department of Homeland Security issued a Final Rule to exempt this system of records from certain provisions of the Privacy Act on August 31, 2009 (74 Fed. Reg. 45069). These regulations remain in effect. This updated system will be included in the DHS inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This revised 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-2012-0045 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

- Fax: 703-483-2999.
- Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

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, visit http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202) 325-0280, CBP Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street, NW, Washington, DC 20229. For privacy issues please contact: Mary Ellen Callahan (703) 235-0780, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) proposes to update and reissue an existing DHS system of records titled, "DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records."

ESTA is a web-based system that DHS/CBP developed in 2008 to determine the eligibility of aliens to travel under the Visa Waiver Program (VWP) to the United States

by air or sea. The authority to collect information required in an ESTA application may be found in Section 217(h)(3) of the Immigration and Nationality Act (INA), 8 U.S.C. § 1187 (h)(3). An eligibility determination under ESTA is made prior to a visitor boarding a carrier en route to the United States, and is accomplished by vetting the information against selected security and law enforcement databases using CBP TECS and the Automated Targeting System (ATS) to determine whether such travel poses a law enforcement or security risk. In addition, ATS retains a copy of ESTA application data to identify potential high-risk ESTA applicants. DHS/CBP previously issued an updated SORN for ESTA on November 2, 2011 (76 Fed. Reg. 67751).

In order to determine whether the applicant is eligible to travel to the United States under the VWP, an applicant provides biographic and other requested information, as well as payment information, using the online application process available at https://esta.cbp.dhs.gov. CBP vets applicant information against various security and law enforcement databases. Payment information is sent to the Department of Treasury's Pay.gov, and CBP a payment status and tracking number in return. CBP is updating the category of records in this system of records to now include the Internet Protocol address (IP address) associated with the submitted ESTA application. As of the effective date of this updated SORN, the IP address will be used as part of the DHS/CBP vetting process. A copy of the application data, including the IP address, will be sent to the ATS in order to identify possible high risk applicants as part of the vetting process.

DHS/CBP is updating this system of records notice to clarify the categories of individuals and remove unnecessary language. DHS/CBP is updating the categories of

records for this system of records notice to permit the collection and use of the IP address associated with an ESTA application. DHS/CBP is also providing more specific legal authorities to collect ESTA information, and clarifying the purposes to include the identification of high-risk applicants.

The routine uses are being updated to add general language ensuring that "[a]ny disclosure of information must be made consistent with the official duties of the person making the disclosure." Routine uses A, D, E, and J are being reworded to provide greater clarity and make non-substantive grammatical changes. Routine use C is being updated to change "other federal government agencies" to "General Services Administration" to better reflect the statutory authorities and the fact that records will be shared with the National Archives and Records Administration (NARA) where NARA maintains the records as permanent records. Routine uses G, K, and M are being reworded to provide greater clarity and remove the now superfluous condition that the "disclosure is appropriate to the proper performance of the official duties of the person making the disclosure." Finally, a new routine use P is being inserted to permit DHS to share this information with 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.

DHS/CBP is also updating this SORN by clarifying the retention of records in ESTA and the Non-Immigrant Information System (NIIS) into which ESTA data may be incorporated based on actual travel to the United States; updating and clarifying the

notification procedures to explain the extension of access procedures to international travelers, allow limited direct access and amendment of ESTA application data, and add the CPB access request address; eliminating unnecessary language from the record source categories describing the use of payment information between ESTA, Pay.gov, and the CBP Credit and Debit Card Data System for payment reconciliation purposes; and clarifying that the Department is exempting the system from sections (c)(3), (e)(8), and (g) of the Privacy Act pursuant to 5 U.S.C. § 552a(j)(2), and is exempting the system from (c)(3) of the Privacy Act pursuant to 5 U.S.C. § 552a(k)(2).

DHS previously published a Final Rule exempting this system of records from certain provisions of the Privacy Act. 74 Fed. Reg. 45069 (Aug. 31, 2009). That Final Rule remains in effect and applicable to this updated system.

The purpose of this system of records is to determine the eligibility of aliens to travel under the VWP to the United States by air or sea. DHS/CBP has authority to operate this system under Title IV of the Homeland Security Act of 2002, 6 U.S.C. § 201, et. seq., and Section 217(h)(3) of the Immigration and Nationality Act, 8 U.S.C. § 1187(h)(3).

Consistent with DHS' information sharing mission, information stored in ESTA may be shared with other DHS components, as well as appropriate federal, state, local, tribal, territorial, foreign, or international government agencies. This sharing will only take place after DHS determines that the recipient has a need to know the information to carry out functions consistent with the exceptions under the Privacy Act of 1974, 5 U.S.C. § 552a(b), and the routine uses set forth in this system of records notice.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which the federal government collects, maintains, uses, and disseminates 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 for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. This system only collects information pertaining to persons in nonimmigrant status, that is, persons who are not covered by the protections of the Privacy Act at the time they provide their information. However, given the importance of providing privacy protections to international travelers, DHS has decided to administratively apply the privacy protections and safeguards outlined in this notice to all international travelers subject to ESTA.

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

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 (ESTA)

Security classification:

Unclassified. The data may be retained on the 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 in the operational system at CBP Headquarters in Washington, D.C. and at CBP 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 foreign nationals who seek to enter the United States by air or sea under the VWP.

Categories of records in the system:

- Full Name (First, Middle, and Last)
- Date of birth
- Gender
- Email address
- Phone number
- Travel document type (e.g., passport), number, issuance date, expiration date and issuing country
- Country of Citizenship
- IP address
- ESTA application number

- 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 Birth
- Date of Anticipated Crossing
- Airline and Flight Number
- City of Embarkation
- Address while visiting the United States (Number, Street, City, State)
- Whether the individual has a communicable disease, physical or mental disorder, or is a drug abuser or addict
- Whether the individual has been arrested or convicted for a moral turpitude crime, drug possession or use, or has been sentenced for a period longer than five years
- Whether the individual has engaged in espionage, sabotage, terrorism or Nazi activity between 1933 and 1945
- Whether the individual is seeking work in the U.S.
- Whether the individual has been excluded or deported, or attempted to obtain a visa or enter U.S. by fraud or misrepresentation
- Whether the individual has ever detained, retained, or withheld custody of a child from a U.S. citizen granted custody of the child
- Whether the individual has ever been denied a U.S. visa or entry into the U.S., or had a visa cancelled, and, if so, the location and date of that denial or

cancellation

- Whether the individual has ever asserted immunity from prosecution
- Any change of address while in the U.S.

Authority for maintenance of the system:

Title IV of the Homeland Security Act of 2002, 6 U.S.C. § 201 et seq.; the INA, 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; and the Travel Promotion Act of 2009, Pub. L. 111-145, 22 U.S.C. § 2131.

Purpose(s):

The purpose of this system is to collect and maintain a record of nonimmigrant aliens who want to travel to the United States under the VWP, and to determine whether applicants are eligible to travel to the United States under the VWP by vetting their information against various security and law enforcement databases and identifying high-risk applicants. This vetting includes consideration of IP address, along with the other application data.

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 Fed. Reg. 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 the operating system on the unclassified and classified DHS networks to allow for analysis and vetting consistent with the above stated 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). Any disclosure of information must be made consistent with the official duties of the person making the disclosure. The routine uses are as follows:

A. To the Department of Justice (DOJ), including the United States Attorney 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 of DHS in his/her official capacity;

3. Any employee of DHS in his/her individual capacity where 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 a written inquiry from that congressional office made pursuant to a Privacy Act waiver from the individual to whom the record pertains.

C. To NARA or the General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906 and for records that NARA maintains as permanent records.

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 harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individuals 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, where 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.

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;

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 with the operations of a DHS component 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 where 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, where 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, but only to the extent that CBP provides information that the ESTA status is not applicable to the traveler, or, if applicable, that the individual is authorized to travel, not authorized to travel, pending, or has not applied.

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, or 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 or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined 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:

Records in this system are stored electronically in the operational system as well as on the unclassified and classified network or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

Retrievability:

These records may be retrieved by any of the data elements supplied by the applicant. The Pay.gov payment tracking number may be used to track the amount of payment associated with an ESTA application and to reconcile payment discrepancies.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and

policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information stored. Access to the computer system containing the records 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, CBP matches 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 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 CBP's financial processing system, CDCDS, pursuant to the DHS/CBP-018, CDCDS system of records notice.

In those instances where a VWP traveler's ESTA data is used for purposes of processing their 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 retained in accordance with the NIIS retention schedule, which is 75 years.

System Manager and address:

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

Notification procedure:

This system only collects information pertaining to persons in nonimmigrant status, that is, persons who are not covered by the protections of the Privacy Act at the time they provide their information. However, given the importance of providing privacy protections to international travelers, DHS has decided to administratively apply the privacy protections and safeguards outlined in this notice to all international travelers subject to ESTA.

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

In addition to using the ESTA system directly to access information provided to DHS/CBP, individuals 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 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. 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 Headquarters or component FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." 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. Requests under the Privacy Act and FOIA

specifically for CBP should be addressed to: U.S. Customs and Border Protection (CBP), Freedom of Information Act (FOIA) Division, 1300 Pennsylvania Avenue, NW Washington, DC 20229.

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

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/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:

The system obtains information from the online ESTA application submitted by the applicant. This information is processed by the Automated Targeting System (ATS) to identify terrorists or threats to aviation and border security, and TECS (for matches to persons identified to be of law enforcement interest), and the vetting result of "authorized to travel," "not authorized to travel," or "pending" is maintained in ESTA. "Pending" will be resolved to "authorized to travel" or "not authorized to travel" based on further research by CBP. Pay.gov provides the Pay.gov tracking number once payment information has been forwarded to it and processed.

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 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.

Dated: July 18, 2012.

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2012-18552 Filed 07/27/2012 at 8:45 am; Publication Date: 07/30/2012]