BILLING CODE: 4410-10

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

DHS-2008-0052

Privacy Act of 1974; Department of Homeland Security, U.S. Customs and Border Protection – Electronic System for Travel Authorization (ESTA), Systems of Records

AGENCY: Privacy Office; Office of the Secretary; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: To provide notice and transparency to the public, the Department of Homeland Security, U.S. Customs and Border Protection announces a new Privacy Act system of records, the Electronic System for Travel Authorization, to collect and maintain a record of nonimmigrant aliens who want to travel to the United States under the Visa Waiver Program (VWP). This new system will determine whether the applicant is eligible to travel to the United States under the VWP by checking their information against various security and law enforcement databases. CBP is publishing a new system of records notice to permit the traveling public greater access to individual information and to provide a more complete understanding of how and where information pertaining to them is collected and maintained.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), the public is given a 30-day period in which to comment on this notice; and the Office of Management and Budget (OMB), which has oversight responsibility under the Act, requires a 40-day period in which to conclude its review of the system. Therefore, the public, OMB, and Congress

are invited to submit comments by [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

- **ADDRESSES:** You may submit comments, identified by DHS-2008-0052 by one of the following methods:
- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 1-866-466-5370.
- Mail: Hugo Teufel III, 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 go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Laurence E. Castelli (202-572-8790), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of International Trade, Regulations & Rulings, Mint Annex, 1300 Pennsylvania Ave., NW, Washington, DC 20229. For privacy issues contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The priority mission of U.S. Customs and Border Protection (CBP) is to prevent terrorists and terrorist weapons from entering the country while facilitating legitimate travel and trade. Upon arrival in the United States, all individuals crossing the border are required to clear CBP. As part of this clearance process, CBP reserves the right to verify the identity, nationality, and determine admissibility of persons traveling to the United States and to create records to assist in this process. Similarly, CBP has authority to keep records of departures from the United States.

CBP does not require that qualifying nationals of countries participating in the VWP present a visa upon their application for admission at a United States port of entry as a nonimmigrant visitor for a period of 90 days or less. As required by Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), DHS/CBP will be implementing an Electronic System for Travel Authorization (ESTA) in order to determine, in advance of departure, whether a traveler is eligible to travel to the United States under the VWP and whether such travel poses a law enforcement or security risk.

Applicants under this program will electronically provide information via an online application prior to traveling to the United States by air or sea. ESTA will store that information in an account. The individual will have the opportunity to verify the accuracy of the information entered in ESTA during the application process and before the application is submitted through ESTA. Applicants will be given a tracking number which, combined with some personal information already provided to the system, will allow the applicant to submit updates to data elements that do not affect their admissibility, or apply for a new ESTA.

Once an applicant has submitted the required information to ESTA, the information supplied by the applicant will be used to automatically query terrorist and law enforcement databases to determine whether the applicant is eligible to travel to the United States under the VWP. When possible matches to derogatory information are found, applications will be vetted through normal CBP procedures. During this time, the applicant will receive a "pending" status. If the applicant is cleared to travel under the VWP, he or she will receive an "authorized to travel" status via the ESTA website. If the applicant is not cleared for travel, the applicant will receive a "not authorized to travel" status and be directed to the State Department website to obtain information on how to apply for a visa at a U.S. consulate or embassy. The Department of State will have access to the information supplied by the applicant and the ESTA results to assist in determining whether to issue a visa.

Carriers, when querying the applicant through the Advance Passenger Information System/APIS Quick Query (APIS/AQQ) system to determine whether a boarding pass should be issued, will be notified whether the applicant traveler has been authorized to travel, not authorized to travel, pending, or has not applied for an ESTA. VWP travelers must have an authorized ESTA or a visa to be issued a boarding pass.

In conjunction with CBP's final rule "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels," which was published in the Federal Register on August 23, 2007 (and became effective on February 19, 2008), DHS has been coordinating with commercial aircraft and commercial vessel carriers on the development and implementation of messaging capabilities for passenger data transmissions that will enable DHS to provide the carriers

with messages pertaining to a passenger's boarding status. A prospective VWP traveler's ESTA status is a component of a passenger's boarding status that has been introduced into the plans for implementing messaging capabilities between DHS and the carriers.

The development and implementation of the ESTA program will eventually allow DHS to eliminate the requirement that VWP travelers complete an I-94W prior to being admitted to the United States. Upon ESTA becoming mandatory, a VWP traveler with valid ESTA will not be required to complete the paper Form I-94W when arriving on a carrier that is capable of receiving and validating messages pertaining to the traveler's ESTA status as part of the traveler's boarding status.

Consistent with DHS's information sharing mission, information stored in the ESTA may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States 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. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system to make agency record keeping practices transparent, to notify individuals regarding the uses to which their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the ESTA system of records.

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

SYSTEM OF RECORDS:

DHS/CBP-009

SYSTEM NAME:

Electronic System for Travel Authorization (ESTA)

SYSTEM CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

This computer database is located at the U.S. Customs and Border Protection (CBP) National Data Center. Computer terminals are located at customhouses, border ports of entry, airport inspection facilities under the jurisdiction of the Department of Homeland Security and other locations at which DHS authorized personnel may be posted to facilitate DHS's mission. Terminals may also be located at appropriate facilities for other participating government agencies, which have obtained system access pursuant to a Memorandum of Understanding.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by ESTA consist of foreign nationals from VWP countries who are seeking to enter the United States by air or sea under the VWP. Under the Immigration and Nationality Act (INA), title 8 of the United States Code, these persons are required to report their arrival and departure to and from the United States. This system only collects information pertaining to persons in non-immigrant 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 apply the privacy protections and safeguards outlined in this notice to all international travelers subject to ESTA.

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
- Date of 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, drugs, 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. (If yes, when and where)
- Whether the individual has ever asserted immunity from prosecution
- Any change of address while in the U.S
- ESTA Tracking Number

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Homeland Security Act of 2002, Pub L. 107-296; 5 U.S.C. § 301 and Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), (Pub. L. 110-53).

PURPOSE:

1) To create a system where foreign nationals of VWP countries may apply for and secure advance authorization to travel to the United States under the VWP;

2) to afford DHS the opportunity to fully screen (vet) the applicant before granting the authorization to travel to the United States under the VWP.

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 to authorized entities, as is determined to be relevant and necessary, outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

A. To an agency, organization, or individual 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;

B. 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) the Department 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 the Department or another agency or entity) or to the individual 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 the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm;

C. 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.

D. To contractors, grantees, experts, consultants, and the agents of thereof, 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;

E. 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);

F. 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 to the proper performance of the official duties of the officer making the disclosure.

G. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws;

H. 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 and such disclosure is proper and consistent with the official duties of the person making the disclosure;

I. To the Department of Justice (including U.S. Attorney offices) or other Federal agencies conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation : (a) DHS or any component thereof, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and

necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

J. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906;

K. 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;

L. To Federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

M. 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;

N. 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 and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

O. To the carrier transporting an individual to the United States, but only to the extent that CBP provides information that the individual is authorized to travel, not authorized to travel, pending, has not applied.

Disclosure to consumer reporting agencies:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

The data is stored electronically at the CBP Data Center for current data and offsite at an alternative data storage facility for historical logs and system backups. Applicants who submit their information online through ESTA will have their information stored in online accounts.

RETRIEVABILITY:

These records may be searched by any of the data elements supplied by the applicant. An admission number, issued at each entry to the United States to track the particular admission, may also be used to identify a database record.

ESTA will not allow applicants to retrieve directly any information from the system, except for their ESTA determination (authorized to travel, not authorized to travel, pending), but will allow the applicant to submit limited updates to data elements that do not affect their admissibility.

SAFEGUARDS:

All ESTA records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include all of the following: restricting access to those with a "need to know"; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications.

ESTA information is secured in full compliance with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including ESTA. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. System users must also complete annual privacy awareness training to maintain current access.

ESTA transactions are tracked and can be monitored. This allows for oversight and audit capabilities to ensure that the data is being handled consistent with all

applicable federal laws and regulations regarding privacy and data integrity. Data exchange, which will take place over an encrypted network between the applicant or a third party submitter on behalf of the applicant, CBP, the carrier industry, Department of State, and other DHS components that have access to the ESTA data, is limited and confined only to those entities that have a need for the data in the performance of official duties. These encrypted networks comply with standards set forth in the Interconnection Security Agreements required to be executed prior to external access to a CBP computer system.

For applicants submitting information to ESTA, access is limited to the online application and the applicant's ESTA determination (authorized to travel, not authorized to travel, pending). Applicants under ESTA do not have access to any other portions of ESTA.

RETENTION AND DISPOSAL:

Information submitted to ESTA generally expires and is deemed "inactive" two years after the last submission or change in 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 will expire concurrently with the passport. Information in ESTA will be retained for one year after the ESTA 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 (3 years active, 12 years archived), to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases, including applications for ESTA that are denied, 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 is in negotiation with NARA for approval of the ESTA data retention and archiving plan.

The ESTA will over time replace the paper I-94W form. In those instances where an ESTA is then used in lieu of a paper I-94W, the ESTA will be maintained in accordance with the retention schedule for I-94W, which is 75 years. I-94W and I-94 data are maintained for this period of time in order to ensure that the information related to a particular admission to the United States is available for providing any applicable benefits related to immigration or other enforcement purposes.

SYSTEM MANAGER(S) AND ADDRESS:

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

NOTIFICATION PROCEDURES:

DHS allows persons (including foreign nationals) to seek administrative access under the Privacy Act to information maintained in ESTA. To determine whether ESTA contains records relating to you, write to the CBP Customer Service Center (Rosslyn VA), 1300 Pennsylvania Avenue NW, Washington, DC 20229; Telephone (877) 227-5511; or through the "Questions" tab at http://www.cbp.gov.xp.cgov/travel/customerservice.

RECORD ACCESS PROCEDURES:

Requests for notification or access must be in writing and should be addressed to the Customer Service Center, OPA - CSC - Rosslyn, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, NW, Washington, DC 20229. Requests should conform to the requirements of 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS and can be found at www.dhs.gov. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Individuals may seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007). Individuals who, for example, believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by a DHS component may submit a redress request through the TRIP. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs such as airports and train stations or when crossing U.S. borders. Through TRIP, a traveler can correct erroneous information stored in DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

CONTESTING RECORD PROCEDURES:

See the "Record Access Procedures" 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 screen for terrorists or threats to aviation and border security) and the Treasury Enforcement Communications System (TECS) (for matches to persons identified to be of law enforcement interest)., and 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 the CBP.

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

Dated:

Hugo Teufel III,

Chief Privacy Officer.

Department of Homeland Security.