



9111-14

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2014-0057]

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: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to update 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 of records allows the U.S. Customs and Border Protection (CBP) at DHS 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 name is provided to DHS as part of a nonimmigrant alien’s ESTA application. The system is used to determine whether the applicant is eligible to travel to and enter the United States under the Visa Waiver Program by vetting the ESTA application information against selected security and law enforcement databases at DHS, including but not limited to the use of CBP’s TECS (not an acronym) and the Automated Targeting System (ATS). In addition, ATS retains a copy of ESTA

application data to identify ESTA applicants who may pose a security risk to the United States. 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 Visa Waiver Program. 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.

As part of the Department's ongoing effort to promote transparency regarding its collection of information, DHS/CBP is updating: (1) the categories of individuals covered by the system, and (2) categories of records in the system to include revised eligibility questions and additional data elements collected on the ESTA application. DHS issued a Final Rule to exempt this system of records from certain provisions of the Privacy Act on August 31, 2009 (74 FR 45070). These regulations remain in effect.

Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will be included in DHS's inventory of systems of records, located on the DHS website at <http://www.dhs.gov/system-records-notices-sorns>.

DATES: This updated system will be effective upon the public display of this notice. Although this system is effective upon publication, DHS will accept and consider comments from the public and evaluate the need for any revisions to this notice.

ADDRESSES: You may submit comments on this notice, including the applicability of the exemptions set forth in the August 31, 2009 Final Rule (74 FR 45070) to the new categories of individuals and categories of records, identified by docket number DHS-2014-0057, 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: Karen L. Neuman, 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, please visit <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: John Connors, (202) 344-1610, CBP Privacy Officer, Privacy and Diversity Office, 1300 Pennsylvania Ave., NW, Washington, D.C. 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, 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) is updating a current DHS system of records titled, “DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records.”

In the wake of the tragedy of September 11, 2001, Congress enacted the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 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 requires 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 since the terrorist attack on the Nation on September 11, 2001, to include more robust security standards that are designed to prevent terrorists and other criminal actors from exploiting the Program to enter the country.

ESTA 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. Applicants submit biographic information and answer eligibility questions using the ESTA website. CBP uses the information submitted to ESTA to make a determination regarding whether the applicant’s intended travel poses a law enforcement or security risk. CBP vets the ESTA applicant information against selected security and law enforcement databases, including the use of TECS and the Automated Targeting System (ATS). ATS also retains a copy of ESTA application data to identify ESTA applicants

who may pose a security risk to the United States. 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 Visa Waiver Program. 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.

The System of Records Notice (SORN) for ESTA, last published on July 30, 2012 (77 FR 44642), is being updated with new categories of individuals and new categories of records to provide notice of new data elements and eligibility questions on the ESTA application. The categories of covered individuals is being updated to accurately reflect information in the system that could pertain to U.S. citizens, U.S. businesses or entities, and lawful permanent residents. The new data elements on the ESTA application provide the Department with enhanced vetting capability while the eligibility questions have been revised to reflect the new data elements and promote readability and make the questions easier to understand by the general public.

Aligning with the 9/11 Commission's recommendation to address the vulnerabilities associated with less stringent screening of VWP travelers, CBP has added the following data elements to the ESTA application to make the screening of VWP

travelers more robust:

- Other Names or Aliases
- Other Country of Citizenship
 - If yes, passport number on additional citizenship passport
- City of Birth
- Home Address
- Parents' Names
- Email Address
- Telephone Number
- National Identification Number
- Current Job Title
- Current or Previous Employer Name
- Current or Previous Employer Address
- Current or Previous Employer Telephone Number
- Emergency Point of Contact Information Name
- Emergency Point of Contact Information Telephone Number
- Emergency Point of Contact Information Email Address
- U.S. Point of Contact Name
- U.S. Point of Contact Address
- U.S. Point of Contact Telephone Number

The addition of these data elements provides additional security in the ESTA application process by enhancing ESTA's vetting capability to identify individuals who

may pose a threat to the United States, thereby reducing the likelihood that an applicant with derogatory security records will be automatically approved for a travel authorization. Moreover, the additional data elements also reduces the number of inconclusive matches to derogatory records during the vetting process, which will decrease the number of applicants who are required to apply for a visa due to ambiguity concerning their identity.

When a person submits an ESTA application, CBP examines the application by screening the applicant's data through ATS (to screen for terrorists or threats to aviation and border security) and TECS (for matches to persons identified to be of law enforcement interest). The additional data elements will help resolve potentially inconclusive matches by providing additional data to confirm an applicant's identity. Inconclusive matches ultimately result in a denial of the ESTA application, which results in an applicant being directed to a U.S. embassy or consulate to apply for a visa.

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's information sharing mission, information stored in ESTA 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. Information stored in ESTA may also be shared with other Federal security and counterterrorism agencies, as well as on a case-by-case basis to appropriate state, local, tribal, territorial, foreign, or international government agencies.

This external sharing takes place after DHS determines that it is consistent with the routine uses set forth in this system of records notice.

Additionally, for ongoing, systematic sharing, DHS completes an information sharing and access agreement with Federal partners to establish the terms and conditions of the sharing, including documenting the need to know, authorized users and uses, and the privacy protections for the data. This updated system will be included in DHS's inventory of systems of records, located on the DHS website at <http://www.dhs.gov/system-records-notices-sorns>.

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, even prior to the collection of these new data elements that may include information about U.S. persons, DHS always administratively applied the privacy protections and

safeguards of the Act to all international travelers subject to ESTA. With the addition of the new data elements, ESTA now falls squarely 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/CBP-009 Electronic System for Travel Authorization (ESTA) 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 (ESTA)

Security classification:

Unclassified. The data may be retained on classified networks but this does not change the nature and character of the data until it is combined with classified information.

System location:

Records are maintained at the CBP Headquarters in Washington, D.C., and in 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. Foreign nationals who seek to enter the United States by air or sea under the VWP; and
2. Persons, including U.S. Citizens and lawful permanent residents, whose information is provided in response to ESTA application questions.

Categories of records in the system:

VWP travelers obtain 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;
- Gender;
- Email address;
- Telephone number (home, mobile, work, other);
- Home address (address, apartment number, city, state/region);
- IP address;
- ESTA application 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;
- Date of anticipated crossing;
- Carrier information (carrier name and flight or vessel number);
- City of embarkation;
- 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;

- Current or previous employer telephone number; and
- Any change of address while in the United States.

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

- Do you currently have any of the following diseases:
 - Chancroid
 - Gonorrhea
 - Granuloma Inguinale
 - Leprosy, infectious
 - Lymphogranuloma venereum
 - Syphilis, infectious
 - Active Tuberculosis
- 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, or 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 you 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?

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; and the Travel Promotion Act of 2009, Public Law 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 and enter the United States under the VWP by vetting their information – and 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 and identifying applicants who pose a security risk to the United States. This vetting includes

consideration of the applicant's 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 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, 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 U.S. 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 U.S. 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;

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 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, 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, 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:

Records may be retrieved 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. 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 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 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.

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 Headquarters, 1300 Pennsylvania Avenue NW, Washington, DC 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. CBP will, however, consider individual requests to determine whether or not information may be released. In processing requests for access to information in this system, CBP will review not only the records in the operational system but also the records that were replicated on the unclassified and classified networks, and based on this notice provide appropriate access to the information.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters 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, SW, 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 Freedom of Information Act Officer, <http://www.dhs.gov/foia> 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; 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:

Records are obtained from the online ESTA application at <https://esta.cbp.dhs.gov/esta/>.

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 routine 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: September 30, 2014.

Karen L. Neuman,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2014-26100 Filed 11/03/2014 at 8:45 am; Publication Date: 11/04/2014]