[Federal Register Volume 80, Number 49 (Friday, March 13, 2015)]
[Notices]
[Pages 13398-13401]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: 2015-05804]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2015-0008]

Privacy Act of 1974; Department of Homeland Security/United States Customs and Border Protection-016 Nonimmigrant and Immigrant Information System

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974 and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of record notices, the Department of Homeland Security (DHS) proposes to update and reissue the following legacy record system, Department of Homeland Security/United States Customs and Border Protection-016 Nonimmigrant Information System. This system of records notice has been updated to include system name, security classification, system location, purpose(s), storage, retention and disposal, and notification procedures. The previous final rule exempts this system from certain aspects of the Privacy Act, and will continue to do so. This notice also 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 Web site at http://www.dhs.gov/system-records-notices-sorns.

DATES: Written comments must be submitted on or before April 13, 2015.

ADDRESSES: You may submit comments, identified by docket number DHS-2015-0008 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, DC 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: John Connors, (202) 344-1610, Privacy Officer, United States Customs and Border Protection, Privacy and Diversity Office, 1300 Pennsylvania Ave. NW., Washington, DC 20229. For privacy questions, please contact: Karen L. Neuman, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) United States Customs and Border Protection (CBP) proposes to update and reissue a current DHS system of records titled, ``DHS/CBP-016 Nonimmigrant Information System System of Records.''

DHS is updating and reissuing a DHS/CBP system of records under the Privacy Act (5 U.S.C. 552a) to reflect CBP's current and future practices regarding the processing of foreign nationals entering the United States. CBP inspects all persons applying for admission to the United States. As part of this inspection process, CBP establishes the identity, nationality, and admissibility of persons crossing the border and may create a border crossing record, which would be covered by DHS/CBP-007 Border Crossing Information System of Records Notice (78 FR 31958, published on May 28, 2013), or additional CBP records, which would be covered by the DHS/CBP-011 TECS System of Records Notice (73 FR 77799, published December 19, 2008) during this process. Similarly, CBP has authority to keep records of departures from the United States.

In addition to information collected from the alien during the inspection process, CBP primarily uses two immigration forms to collect information from nonimmigrant aliens as they arrive in the United States: The I-94, Arrival/Departure Record; and the I-94W, Nonimmigrant Visa Waiver Arrival/Departure Form (for aliens applying for admission under the visa waiver program (VWP)). Separately, Canadian nationals that travel to the U.S. as tourists or for business and Mexican nationals who possess a nonresident alien Mexican Border Crossing Card are not required to complete an I-94 upon arrival. However, their information is maintained in Nonimmigrant and Immigrant Information System (NIIS). Additionally, DHS/CBP implemented an Electronic System for Travel Authorization (ESTA) to permit nationals of VWP countries to submit their biographic and admissibility information online in advance of their travel to the United States. Applicants under this program will have access to their accounts so that they may check the status of their ESTA and make limited amendments. ESTA is covered by privacy documentation including the DHS/CBP Electronic System for Travel Authorization SORN (79 FR 65414, published on November 3, 2014).

In accordance with the Privacy Act of 1974 and as part of DHS's ongoing effort to review and update legacy system of record notices, DHS/CBP proposes to update and reissue the following system of records notice, DHS/CBP-016 Nonimmigrant and Information System (73 FR 77739, published December 19, 2008), as a DHS/CBP system of records notice titled, DHS/CBP-016 Nonimmigrant and Immigrant Information System System of Records. DHS/CBP changed the system name to reflect changes to the system, changed the security classification to reflect storage of records on a classified network, changed the system location to reflect a new location, changed the purpose to allow for replication of data for analysis and vetting, updated the storage due to the change in security classification, updated the retention and disposal to reflect that records will follow the same retention schedule, and changed the notification procedure to reflect that DHS/CBP will now also review replicated records.

Consistent with DHS's information sharing mission, information stored in the DHS/CBP-016 Nonimmigrant and Immigrant Information System System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies

[[Page 13399]]

consistent with the routine uses set forth in this system of records notice.

Additionally, the exemptions for this system of records notice will remain in place. This updated system will be included in the DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the 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 the 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.

Below is a description of the DHS/CBP-016 Nonimmigrant and Immigrant Information System System of Records.

In accordance with 5 U.S.C. 552a(r), a report concerning this record system has been sent to the Office of Management and Budget and to the Congress.

System of Records:

Department of Homeland Security DHS/United States (U.S.) Customs and Border Protection (CBP)-016.

System Name:

DHS/CBP-016 Nonimmigrant and Immigrant Information System.

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, DC and at CBP field offices. Records are replicated from the operational system and maintained on the DHS unclassified and classified networks. 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 that have obtained system access pursuant to a Memorandum of Understanding.

Categories of Individuals Covered by This System:

Categories of individuals covered by this system are nonimmigrant aliens entering and departing the United States.

Categories of Records in This System:

The Nonimmigrant and Immigrant Information System (NIIS) is a dataset residing on the CBP Information Technology (IT) platform and in paper form. It contains arrival and departure information collected from foreign nationals entering and departing the United States on such forms as the I-94 and I-94W, or through interviews with CBP officers. This information consists of the following data elements, as applicable:

Full Name (first, middle, and last);

Date of birth;
Email address, as required;
Travel document type (e.g., passport information, permanent resident card), number, issuance date, expiration date and issuing country;
Country of citizenship;
Date of crossing both into and out of the United States;
Scanned images linked through the platform;
Airline and flight number;
City of embarkation;
Address while visiting the United States;
Admission number received during entry into the United States;
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 United States;
Whether the individual has been excluded or deported, or attempted to obtain a visa or enter the United States 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; and
Any change of address while in the United States.

Authority for Maintenance of the System:

The legal authority for NIIS comes from the Immigration and Nationality Act, 8 U.S.C. 1103, 1184, 1354; the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458; the Homeland Security Act of 2002, Public Law 107-296; 5 U.S.C. 301; and the Federal Records Act, 44 U.S.C. 3101.

Purpose(s):

NIIS is a repository of records for persons arriving in or departing from the United States as nonimmigrant visitors and is used for entry screening, admissibility, and benefits purposes. The system provides a central repository of contact information for such aliens while in the United States and also captures arrival and departure information for determination of future admissibility.

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) as follows:

A. To the Department of Justice (DOJ), including Offices of the United States Attorney or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

[[Page 13400]]

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. The Department 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 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.

I. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

J. 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.

K. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a

requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

L. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for the purpose of protecting the vital 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).

M. To federal and foreign government intelligence or counterterrorism agencies or components when CBP becomes aware of an indication of a threat or potential threat to national or international security, or when 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.

N. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations when DHS is aware of a need to use relevant data for purposes of testing new technology and systems designed to enhance national security or identify other violations of law.

O. 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 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 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. DHS/CBP stores the records on magnetic disc, tape, digital media, and CD-ROM. The data is stored electronically at the CBP and DHS Data Center for current data and offsite at an alternative data storage facility for historical logs, system backups, and in paper form.

Retrievability:

These records may be searched on a variety of data elements including name, addresses, place and date of entry or departure, or country of citizenship as listed in the travel documents used at the time of entry to the United States. 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.

Safeguards:

All NIIS 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.

NIIS information is secured in full compliance with the requirements of the

[[Page 13401]]

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 NIIS. 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.

NIIS 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.

Retention and Disposal:

NIIS data is subject to a retention requirement. The information collected and maintained in NIIS is used for entry screening, admissibility, and benefits purposes and is retained for seventy-five (75) years from the date obtained. However, NIIS records that are linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases will remain accessible for the life of the law enforcement activities to which they may become related. The current disposition for paper copy is 180 days from date of departure. Records replicated on the unclassified and classified networks will follow the same retention schedule.

System Manager and address:

Assistant Commissioner, Office of Information Technology, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue NW., Washington, DC 20229.

Notification procedure:

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 CBP's FOIA Officer, 1300 Pennsylvania Avenue NW., Washington, DC 20229.

When seeking records about yourself from this system of records or any other CBP 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 Director, Disclosure and FOIA, 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; 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/her agreement for you to access his/her records.

Without this bulleted information CBP 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.

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.

Record access procedures:

See ``Notification procedure'' above.

Contesting record procedures:

See ``Notification procedure'' above.

Record source categories:

The system contains certain data received on individuals, passengers and crewmembers that arrive in, depart from, or transit through the United States. This system also contains information collected from carriers that operate vessels, vehicles, aircraft, and/or trains that enter or exit the United States and from the individuals upon crossing the U.S. border.

Basic information is obtained from individuals, the individual's attorney/representative, CBP officials, and other federal, state, local, and foreign agencies.

Exemptions claimed for the system:

No exemption shall be asserted with respect to information maintained in the system that is collected from a person or submitted on behalf of a person, if that person, or his or her agent, seeks access or amendment of such information.

This system, however, may contain information related to an ongoing law enforcement investigation because the information regarding a person's travel and border crossing was disclosed to appropriate law enforcement in conformance with the above routine uses. As such pursuant to 5 U.S.C. 552a(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: February 27, 2015.

Karen L. Neuman,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2015-05804 Filed 3-12-15; 8:45 am]
BILLING CODE 9111-14-P