[Federal Register Volume 77, Number 153 (Wednesday, August 8, 2012)]
[Notices]
[Pages 47411-47415]
From the Federal Register Online via the Government Publishing Office [www.gpo.gov]
[FR Doc No: 2012-19337]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0018]

Privacy Act of 1974; Department of Homeland Security/U.S. Citizenship and Immigration Services--006 Fraud Detection and National Security Records, 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, 5 U.S.C. 552a, the Department of Homeland Security proposes to update and reissue the Department of Homeland Security system of records notice currently titled,'' Department of Homeland Security/U.S. Citizenship and Immigration Services--006 Fraud Detection and National Security Data - System and renaming it Fraud Detection and National Security Records.'' This system of records assists the Department of Homeland Security/U.S. Citizenship and Immigration Services in performing its statutory missions including strengthening the integrity of the nation's legal immigration system by ensuring that immigration benefits are not granted to individuals that may pose a threat to national security and/or public safety. In addition, this system of records assists the Department of Homeland Security/U.S. Citizenship and Immigration Services' recording, tracking, and managing immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns. This system of records is being updated to more clearly describe the functions of the Fraud Detection and National Security Directorate and clarify that the system of records contains both electronic and paper files.

DATES: Submit comments on or before September 7, 2012. This revised system will be effective September 7, 2012.

ADDRESSES: You may submit comments, identified by docket number DHS-2012-0018 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: Mary Ellen Callahan, 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: United States Citizenship and Immigration Services, Privacy Officer, Donald Hawkins (202-272-8000), 111 Massachusetts Avenue NW., Washington, DC 20529. For privacy issues please contact: Mary Ellen

[[Page 47412]]

Callahan (202-343-4010), Chief Privacy Officer, Privacy Office, U.S. 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)/U.S. Citizenship and Immigration Services (USCIS) proposes to update and reissue the DHS system of records currently titled, ``Department of Homeland Security/U.S. Citizenship and Immigration Services--006 Fraud Detection and National Security Data System System of Records'' (last published August 18, 2008, 73 FR 48231) and renaming it Fraud Detection and National Security Records. This system of records notice (SORN) is being updated to better describe the functions of the Fraud Detection and National Security Directorate (FDNS).

DHS through USCIS implements immigration law and policy through the processing and adjudication of applications and petitions submitted for citizenship, asylum, and other immigration benefits. Benefits may include adjustment of immigration status (granting lawful permanent residence), naturalization (granting United States citizenship), asylum and refugee status, and other immigrant and nonimmigrant benefits. USCIS supports the DHS statutory mandate of protecting the nation by identifying applicants who threaten national security or public safety and denying them immigration benefits that would allow them to legally enter or remain in the United States. In addition, USCIS enhances the integrity of the nation's legal immigration system by detecting and deterring immigration benefit fraud. In order to support this DHS statutory mandate, USCIS collects applicant, petitioner, and beneficiary information to adjudicate applications and petitions so that immigration benefits are only granted to eligible individuals in an accurate, efficient, and timely manner. This information is also used to determine if and when those benefits should be rescinded or revoked.

In 2004, USCIS established FDNS in response to a Congressional recommendation to establish an organization ``responsible for developing, implementing, directing, and overseeing the joint USCIS-U.S. Immigration and Customs Enforcement (ICE) anti-fraud initiative and conducting law enforcement/background checks on every applicant, beneficiary, and petitioner prior to granting immigration benefits.'' FDNS fulfills the USCIS mission of enhancing both national security and the integrity of the legal immigration system by: (1) Identifying threats to national security and public safety posed by those seeking immigration benefits; (2) detecting, pursuing, and deterring immigration benefit fraud; (3) identifying and removing systemic vulnerabilities in the process of the legal immigration system; and (4) acting as USCIS's primary conduit for information sharing and collaboration with other governmental agencies. FDNS also oversees a strategy to promote a balanced operation that distinguishes USCIS's administrative authority, responsibility, and jurisdiction from ICE's criminal investigative authority.

FDNS serves as the primary liaison between USCIS and the law enforcement and intelligence communities. This effort includes establishing and developing relationships and collaborating with law enforcement, intelligence, and federal, state, and local agencies to ensure criminals, terrorists, and other individuals who pose a threat to national security and/or public safety are not able to exploit the immigration system to gain access to, or remain in, the United States. In addition, FDNS works with Immigration Services Officers (ISOs) on cases of suspected fraud and where the security vetting process has indicated possible national security or public safety-related concerns.

FDNS uses Fraud Detection and National Security Data System (FDNS-DS) to record, track, and manage the background check process related to immigration applications and petitions, as well as information related to beneficiary applications with suspected or confirmed fraud, criminal activity, public safety and/or national security concerns, and cases randomly selected for benefit fraud assessments. FDNS-DS maintains information on all individuals who have been reviewed for these concerns. In instances where no fraud, criminal activity, public safety and/or national security concerns were found, the information maintained will only be used to demonstrate that an assessment was conducted so additional resources do not have be used for a second review.

FDNS may share FDNS records with law enforcement and intelligence agencies in response to Requests for Information (RFIs) to support criminal and administrative investigations and background checks involving immigrant benefit fraud, criminal activity, and public safety and/or national security concerns. For example, information may be shared with the Department of State (DoS), Bureau of Consular Affairs to provide a comprehensive picture of a visa applicant's status, and to reduce the likelihood that an individual or group might fraudulently obtain an immigration benefit under the Immigration and Nationality Act (INA), as amended. Also, selected ICE representatives have access to certain FDNS records for purposes of criminal investigations. This system of records notice covers not only those records maintained in FDNS-DS, but also those maintained in other IT systems developed specifically for FDNS, such as a collaborative workspace, and paper files. The controls and rules associated with the data remain consistent across these different physical types of records.

Separately, DHS is publishing a Privacy Impact Assessment (PIA) on the functions of FDNS, which can be found at www.dhs.gov/privacy.

USCIS is republishing this SORN to provide public notice of the following: (1) The name of the system has been updated to FDNS Records to reflect that it covers not only records in FDNS-DS but also other information technology systems created specifically for FDNS and paper records; (2) location of the system has been updated to include not only FDNS-DS but the records maintained in collaborative workspaces and paper files; (3) categories of individuals has been updated to clarify that this system only covers those who are or have been the subject of an inquiry; (4) categories of records has been updated to clarify what information may be collected on Representatives and Preparers in the system when there are indicia of fraud or national security concerns connected with their appearance before USCIS; (5) authorities under which this system runs have been updated; (6) routine uses have been updated with minor changes to be consistent with other DHS systems of records; and (7) sources of records have been updated to include publicly available information on the Internet.

Previously, DHS issued a final rule published on August 31, 2009 at 6 CFR part 5, appendix C, paragraph 32 exempting this system from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). The updates to this SORN do not necessitate a republication of the exemptions. As noted in the final rule to the extent FDNS maintains a record received from a law enforcement system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions. This updated system

[[Page 47413]]

will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which 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. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents (LPRs). As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, LPRs, 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 in order to make agency record keeping practices transparent, to notify individuals regarding the uses of their record, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/USCIS-006 FDNS SORN.

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

DHS/USCIS-006

System name:

DHS/USCIS-006 Fraud Detection and National Security Records.

Security classification:

Unclassified.

System location:

Records are maintained in the IT system FDNS-DS, other information technology systems developed to support FDNS, and paper files at the USCIS Headquarters in Washington, DC and field offices.

Categories of individuals covered by the system:

Categories of individuals covered by this system include: (1) Individuals who are the subjects of administrative and/or criminal investigations; (2) individuals who have submitted potentially fraudulent petitions and applications for immigration benefits; (3) individuals whose petitions or applications have been randomly selected for assessment of the effectiveness of fraud detection programs; (4) individuals of concern based on possible national security reasons, public safety concerns, or criminal activity; (5) preparers, representatives, and petitioning organizations that may have submitted applications or petitions on behalf of individuals noted in the above four categories; (6) individuals who are associated with an application but are not actually applying for a benefit; and (7) individuals associated with cases that were investigated but determined not to pose any concern.

Categories of records in the system:

Categories of records in this system include:

Individual's name;
Alias(es);
Social Security Number (SSN);
Alien Number (A-Number);
Associated A-Numbers of close relatives and associates;

Application Receipt Number;

Address (home and business);

Date of birth;

Place of birth;

Driver's License number;

Country of citizenship;

Citizenship status;

Gender;

Telephone number(s);

Email address;

Place of employment and employment history;

Associated organizations (e.g., corporate information relating to employing entity if employment-based immigration benefits are being sought, and place of business or place of worship if such organization is sponsoring the applicant);

Family lineage;

Bank account information and/or financial transaction history;

Marriage record;

Civil or criminal history information;

Information on social media Web sites and other information publicly available on the Internet;

Education record;

Information from commercial data providers in order to verify information provided on the application;

Biometric identifiers (e.g., photographic facial image, fingerprints, signature, etc);

Investigation or background check information generated by DHS/CBP TECS National Crime Information Center, other government agencies, and other data and analysis generated as part of the adjudication process;

Other unique identifying numbers or characteristics such as passport number(s), visa number(s), account numbers, and other identifiers associated with travel; and

Representative and Preparer information maintained in the G-28, Notice of Entry of Appearance as an Attorney or Accredited Representative

[cir] Name
[cir] Address
[cir] Phone number
[cir] Fax number
[cir] Email address
[cir] Bar number
[cir] State of bar membership
[cir] Date of filing
[cir] Associated client case information

Note: FDNS may gather additional data on Representatives or Preparers that are the subject or associated with a fraud, public safety, or national security concern based on applications submitted on behalf of individuals seeking an immigration benefit.

Authority for maintenance of the system:

The Immigration and Nationality Act of 1952, as amended (INA), 8 U.S.C. 1101, et seq. provides the legal authority to collect information used for the adjudication of immigration benefits. In addition to other delegations, the Secretary of Homeland Security in Homeland Security Delegation No. 0150.1 paragraphs (H), (I), (J), (M), and (S) has delegated the following authorities to USCIS:

Authority under section 103(a)(1) of the INA, 8 U.S.C. 1103(a)(1), to administer the immigration laws (as defined in section 101(a)(17) of the INA).

Authority to investigate alleged civil and criminal violations of the immigration laws, including but not limited to alleged fraud with respect to applications or determinations within the

Bureau of Citizenship and Immigration Services (BCIS) [predecessor to USCIS] and make recommendations for prosecutions or other appropriate action when deemed advisable.

Authority to fingerprint and register aliens.

Authority to maintain files and records systems as necessary.

Authority to take and consider evidence.

In addition, the joint USCIS-ICE anti-fraud strategy was recommended by the Conference Report, FY 2005 Appropriations Act. The Appropriations Act authorized USCIS to conduct law enforcement and background checks on every applicant, beneficiary, and petitioner prior to granting immigration benefits.

[[Page 47414]]

Purpose(s):

The purpose of this system is to support USCIS' efforts to strengthen the integrity of the nation's legal immigration system and to ensure that immigration benefits are not granted to individuals who may pose a threat to national security and/or public safety. In addition, FDNS is responsible for detecting, deterring, and combatting immigration benefit fraud.

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 (including 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 the National Archives and Records Administration 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 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 who 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 and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To federal and foreign government intelligence or counterterrorism agencies when USCIS 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.

I. 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.

J. 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 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:

Records may be retrieved by utilizing multiple data points that include an individual's last name, A-Number, Application Receipt Number, Date of Birth, or other unique identifier.

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 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. FDNS-DS maintains a real-time auditing function of individuals who access the system.

Retention and disposal:

FDNS records have a retention period of 15 years from the date of the last interaction between FDNS personnel and the individual after which time the record will be deleted from FDNS. The 15-year retention schedule provides FDNS with access to information that is critical to the investigation of suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns. Upon closure of a case, any information that is needed to make an adjudicative decision (such as a statement of findings report), whether there was or was not an indication of fraud, criminal activity, egregious public safety, and/or national security concerns, will be transferred to the A-File and maintained under the A-File

[[Page 47415]]

retention period of 100 years after the individual's date of birth.

System Manager and address:

Associate Director of FDNS, United States Citizenship and Immigration Services, 111 Massachusetts Avenue NW., Washington, DC 20529.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, amendment, and certain accounting procedures of the Privacy Act. These exemptions also apply to the extent that information in this system of records is recompiled or is created from information contained in other systems of records. As noted below, where a record received from a law enforcement system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions in accordance with this rule. 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 National Records Center, FOIA/PA Office P.O. Box 648010 Lee's Summit, MO 64064-8010. 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, Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP-0655, Washington, DC 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 Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide:

Provide an explanation of 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 seeks 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 bulleted information DHS 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:

Parties who file USCIS applications supply the basic information contained in this system. Other information comes from petitions, law enforcement and intelligence agencies, public institutions, interviews of witnesses, public records, sworn statements, official reports, commercial data aggregators, publicly available information on the Internet, and from members of the general public.

Exemptions claimed for the system:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2): 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Additionally, many of the functions in this system require retrieving records from law enforcement systems. Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions in accordance with this rule.

Dated: July 31, 2012.
Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2012-19337 Filed 8-7-12; 8:45 am]
BILLING CODE 9111-97-P