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 DHS or another agency or entity) or harm to the individual who relies 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 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 are retrieved by individual's name, business' name, addresses, telephone number, account number, or order number.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated system security 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.

RETENTION AND DISPOSAL:

Flood plain Management Files end at the close of each fiscal year, retired to the Federal Record Center, and destroyed ten years after cutoff, in accordance with FEMA Records Schedule N1–311–02–01, Item 4. Files generated in processing flood insurance policies under the continuing National Flood Insurance Program end when file becomes inactive and destroyed five years after cutoff, in accordance with FEMA Records Schedule N1–311–86–1, Item 1A13a(2).

SYSTEM MANAGER AND ADDRESS:

Administrator, Federal Insurance and Mitigation Administration, Federal Emergency Management Agency Headquarters, 500 C Street, SW., Washington, DC 20472.

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 FEMA's FOIA Officer, 500 C Street, SW., Attn: FOIA Coordinator, Washington, DC 20472.

When seeking records about yourself from this system of records or any other FEMA 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 the following:

- An explanation of why you believe the Department would have information on you,
- Specify when you believe the records would have been created,
- 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 the FEMA 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:

Individual's who apply for and individuals who are insured under the National Flood Insurance Program, Write-Your-Own companies, flood insurance agents and lenders, and individuals who request information on the National Flood Insurance Program.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29812 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0162]

Privacy Act of 1974; United States Citizenship and Immigration Services—008 Refugee Access Verification Unit System of Records.

AGENCY: Privacy Office; DHS.

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 records notices, the Department of Homeland Security is giving notice that it proposes to update and reissue the following legacy record system, Justice/INS–006 Refugee Access Verification Unit Records, December 26, 2002, as a Department of Homeland Security U.S. Citizenship and Immigration Services system of records titled, U.S. Citizenship and Immigration Services Refugee Access Verification Unit System of Records.

The identification of potential refugees and the initial processing of potential refugees is performed by the Department of State, outside of the United States, and information associated with this process is captured in the Department of States' Worldwide Refugee Processing System. Although the Department of Homeland Security U.S. Citizenship and Immigration Services has limited access to the system, it does not belong to Department of Homeland Security U.S. Citizenship and Immigration Services. There are four categories of fact patterns under which an individual can become eligible for resettlement in the United States as a refugee. The Department of Homeland Security U.S. Citizenship and Immigration Services has a separate system that contains information related to only one of these categories, which is when a family member in the United States files an Affidavit of Relationship. Information related to the other three categories is initially captured in the Department of States' Worldwide Refugee Processing System and then in the Department of Homeland Security U.S. Citizenship and Immigration Services' DHS–USCIS–001 A-File system (72 FR 1755 January 16, 2007) after the individual comes to the United States. In addition, information related to individuals for whom Affidavits of Relationships have been filed may also be captured in Department of Homeland Security U.S. Citizenship and Immigration Services' DHS–USCIS–007 Benefits Information System (73 FR 56596, September 29, 2008) as the applicant seeks to adjust his or her status.

Categories of individuals, categories of records and routine uses and purpose of this legacy system of records notice have been updated to better reflect the United States Citizenship and Immigration Services' Refugee Access Verification Unit records. Additionally, authorities for maintenance of the system, retention and disposal, and system manager have been updated to reflect the systems current operations. This updated system of records notice will be included in the Department of Homeland Security's inventory of record systems.

DATES: Written comments must be submitted on or before January 20, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0162 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, 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 and may be read at *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 Donald K. Hawkins (202–272–8404), Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue, NW., Washington, DC 20529. For privacy issues please 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

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107–296, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and the U.S. Citizenship and Immigration Services (USCIS) have relied on preexisting Privacy Act systems of records notices for the collection and maintenance of records handled by USCIS Refugee Access Verification Unit (RAVU).

As part of its efforts to streamline and consolidate its record systems, DHS is updating and reissuing a USCIS system of records under the Privacy Act (5 U.S.C. 552a) that deals with storing and reporting the results of the Affidavit of Relationship (AOR) review for refugee applicants. This record system allows DHS/USCIS to collect and preserve the records regarding the processing of AORs for potential refugee applicants. The collection and maintenance of this information will assist DHS/USCIS in accomplishing the following three functions: (1) Issuing its findings to the Department of State (DOS) in furtherance of the DOS' onward processing outside of the United States; (2) to permit the return of the AOR to the anchor relative due to a finding of ineligibility and; (3) to assist USCIS in tracking statistics regarding findings of fraud.

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 records notices, the Department of Homeland Security is giving notice that it proposes to update and reissue the following legacy record system, Justice/INS–006 Refugee Access Verification Unit Records, December 26, 2002, as a Department of Homeland Security U.S. Citizenship and Immigration Services system of records titled, U.S. Citizenship and Immigration Services Refugee Access Verification Unit System of Records.

The identification of potential refugees and the initial processing of potential refugees is performed by the Department of State, outside of the United States, and information associated with this process is captured in the Department of States' Worldwide Refugee Processing System. Although the Department of Homeland Security U.S. Citizenship and Immigration Services has limited access to the system, it does not belong to Department of Homeland Security U.S. Citizenship and Immigration Services. There are four categories of fact patterns under which an individual can become eligible for resettlement in the United States as a refugee. The Department of Homeland Security U.S. Citizenship and Immigration Services has a separate system that contains information related to only one of these categories, which is when a family member in the United States files an Affidavit of Relationship. Information related to the other three categories is initially captured in the Department of States' Worldwide Refugee Processing System and then in the Department of Homeland Security U.S. Citizenship and Immigration Services' DHS–USCIS–001 A-File system (72 FR 1755, January 16, 2007) after the individual comes to the United States. In addition, information related to individuals for whom Affidavits of Relationships have been filed may also be captured in Department of Homeland Security U.S. Citizenship and

Immigration Services' DHS–USCIS–007 Benefits Information System (73 FR 56596, September 29, 2008) as he or she seeks to adjust his or her status.

Categories of individuals, categories of records and routine uses and purpose of this legacy system of records notice have been updated to better reflect the United States Citizenship and Immigration Services' Refugee Access Verification Unit records. Additionally, authorities for maintenance of the system, retention and disposal, and system manager have been updated to reflect the systems current operations. This updated system of records notice will be included in the Department of Homeland Security'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 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 lawful 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.

In addition, information pertaining to an individual's status as a refugee is as a matter of DHS policy, afforded the confidentiality protections contained in 8 CFR 208.6 which strictly limits the disclosure of information to third parties.

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 records, and to assist individuals to more easily find such files within the agency. Below is the description of the Protected Status Application Information System of Records.

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

System of Records DHS/USCIS–008

SYSTEM NAME:

United States Citizenship and Immigration Services Refugee Access Verification Unit Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at the United States Citizenship and Immigration Services Headquarters, Refugee Affairs Division in Washington, DC, and field locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include priority three (P3) refugee applicants and their relatives who have not yet received a refugee classification interview by DHS/USCIS; and anchor relatives such as lawful permanent residents and/or United States citizen relatives in the United States who have filed an Affidavit of Relationship (AOR) on behalf of a refugee applicant overseas under the P3 worldwide processing priorities.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system may include:

- Applicant's name and the name of accompanying family members and their contact information;
- Anchor's Alien number (if applicable);
- Anchor relative's name and contact information;
- Interview worksheets;
- Other applications for USCIS benefits and related forms;
- AOR and AOR review checklists and decision notices;
- Biographic and demographic information of anchor relative and applicant such as family trees and documents establishing identity;
- Communication from voluntary agencies; Members of Congress; U.S. Government agencies and International organizations;
- AOR Review findings;
- Case number.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; the Federal Records Act, 44 U.S.C. 3101; 8 U.S.C. 1522(b) (Authorization for Programs for Initial Domestic Resettlement of and Assistance to Refugees) and 8 U.S.C. 1157 (Annual Admission of Refugees and Admission of Emergency Situation Refugees).

PURPOSE(S):

The purpose of this system is to track and manage the review of Affidavits of Relationship (AORs) filed by anchor relatives in the United States on behalf of certain family members overseas seeking consideration for refugee resettlement under Priority Three (P3) to the United States.

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 of 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 or other Federal agency 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:

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, 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.

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 or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. 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.

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 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 individual who relies 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 the Department of State (DOS), when necessary to accomplish an agency function related to this system of records.

I. To an attorney or representative who is acting on behalf of an individual covered by this system of records (as defined in 8 CFR 1.1(j)) in conjunction with any proceeding before DHS/USCIS or the Executive Office for Immigration Review.

J. To a former employee of the Department for purposes of responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

K. To Federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or where 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.

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 and on paper in secure facilities in a locked drawer behind a locked door.

RETRIEVABILITY:

Records may be retrieved by refugee applicant's name, refugee alien number, case number, and anchor relative's name.

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.

RETENTION AND DISPOSAL:

In accordance with National Archives and Records Administration approved schedule N1–563–04–5, the RAVU electronic master file records are maintained 20 years before destruction; case files are maintained at USCIS Headquarters for 2 years and then destroyed.

SYSTEM MANAGER AND ADDRESS:

Chief, Refugee Affairs Division, Refugee, Asylum and International Operations Directorate, 111 Massachusetts Avenue, Eighth Floor, Washington, DC 20529.

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 National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO 64064–8010. Specific FOIA contact information can be found at *http://www.dhs.gov/foia* under ''contacts.''

When seeking records about yourself from this system of records or any other USCIS 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 the following:

- An explanation of why you believe the Department would have information on you,
- Specify when you believe the records would have been created,
- 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 USCIS 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:

Information contained in this system of records is obtained from the individual who is the subject of these records as well as relatives, sponsors, Members of Congress, U.S. Government agencies, voluntary agencies, international organizations, and local sources at overseas posts.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, U.S. Department of Homeland Security.

[FR Doc. E8–29837 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P