persons and organizations is essential to detecting criminal and terrorist patterns of behavior and locating leads in current investigations, ICE has proposed to retain records in ICEPIC for ten (10) years from ICE's last use of the individual's data, and then archive the information for an additional five (5) years. After the five (5) year period, information will be destroyed unless it has become relevant to a legal action, at which point the retention schedule would reset.

SYSTEM MANAGER(S) AND ADDRESS:

Unit Chief, Program Management Oversight, Mission Support, Office of Investigations, U.S. Immigration and Customs Enforcement, 425 I Street, NW., Washington, DC 20536, telephone: (202) 307–6201.

NOTIFICATION PROCEDURES:

Pursuant to 5 U.S.C. 552a(j) and (k), this system of records may not be accessed by members of the public for purposes of determining if the system contains a record pertaining to a particular individual. Nonetheless persons may seek access to records maintained in ICEPIC as outlined in the Record Access Procedures section below. Requests for such access will be reviewed on a case-by-case basis.

RECORD ACCESS PROCEDURES:

ICEPIC is exempt from record access procedures pursuant to 5 U.S.C. 552a(j) and (k). Nonetheless persons may seek access to records maintained in ICEPIC by contacting U.S. Immigration and Customs Enforcement Freedom of Information Act Office, 800 North Capitol Street, NW., Room 585, Washington, DC 20536. Individuals must submit their request and use the form found at *http://www.ice.gov/doclib/g-639.pdf*. Requests for such access will be reviewed on a case-by-case basis to ensure that the records meet the requirements set out by the Privacy Act.

CONTESTING RECORD PROCEDURES:

This system is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4) (G) and (H), and (f) pursuant to 5 U.S.C. 552a(j)(2), (k)(2); however, requests for amendment of records may be reviewed on a case-by-case basis. Follow the ''Record Access Procedures'' noted above.

RECORD SOURCE CATEGORIES:

Information contained in the system is obtained from DHS investigators, other DHS law enforcement officers, other Federal, State, foreign and tribal law enforcement and intelligence agencies, public records, commercial data aggregators, and immigration and alien admission records systems.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to exemption 5 U.S.C. 552a(j)(2) of the Privacy Act, portions of this system are exempt from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f), and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). In addition, to the extent a record contains information from other exempt systems of records, ICE will rely on the exemptions claimed for those systems.

Dated: August 11, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–19031 Filed 8–15–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2007–0054]

Privacy Act of 1974; United States Citizenship and Immigration Services; Fraud Detection and National Security Data System (FDNS–DS) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: The USCIS has developed the Fraud Detection and National Security Data System (FDNS–DS), a case management system used to record, track, and manage immigration inquiries, investigative referrals, law enforcement requests, and case determinations involving benefit fraud, criminal activity, public safety and national security concerns.

DATES: Written comments must be submitted on or before September 17, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS–2007–0054 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 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, 111 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

The Office of Fraud Detection and National Security (FDNS) of the United States Citizenship and Immigration Services (USCIS) has developed a new system named the Fraud Detection and National Security Data System (FDNS–DS). FDNS–DS is a central repository that permits specially-trained employees to record, track, and manage the background checks and adjudicative processes related to immigration applications and petitions with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns, and cases randomly selected for benefit fraud assessments (BFAs). The system will also have the capability to track the following:

1. USCIS investigative referrals to law enforcement agencies (LEAs);
2. LEA referrals to USCIS concerning subjects with pending immigration benefit applications or petitions;
3. background check referrals and resolutions associated with suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns; and
4. any additional inquiries conducted in order to confirm that the information on file is correct.

FDNS has created FDNS–DS, a centralized data system, in order to increase the effectiveness of United States (U.S.) immigration system in identifying threats to national security, combating benefit fraud, and locating and removing vulnerabilities that compromise the integrity of the legal immigration system. With the implementation of FDNS–DS, USCIS's capabilities for detecting and tracking

benefit fraud and other criminal activity—and conducting efficient and accurate background check resolutions and adjudication of national security cases will be increased.

In order to achieve the goals discussed above, FDNS–DS will store data related to immigration applications involving suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns. The data will include the results of required background checks conducted in connection with pending petitions/applications that results in subsequent inquiries conducted to resolve the background check results. FDNS–DS will also contain the following information related to cases involving suspected or confirmed fraud, criminal activity, egregious public safety, and/or national security concerns: USCIS investigative referrals to law enforcement agencies (LEAs) of suspected or confirmed fraud or other criminal activity; LEA referrals to USCIS related to pending applications; referrals to USCIS from the public or other governmental entities or fraud case referrals from the Benefit Fraud Assessment (BFA) process (''other referrals''); adverse information identified by USCIS from applications, administrative files, interviews, written requests for evidence (RFEs) or site visits; results of resolution of any of the above-described categories of adverse information; and adjudicative summaries and decisions.

As noted above, FDNS–DS will store information concerning cases randomly selected for BFAs and will track interactions with Immigration and Citizenship Enforcement (ICE) and other LEAs (*e.g.*, the Federal Bureau of Investigation [FBI], the Drug Enforcement Administration [DEA], and U.S. Customs and Border Protection [CBP]) in cases involving fraud or other criminal activity, and the Department of State in cases involving fraud related to selected types of visas for entry into the United States.

USCIS may elect to withhold any related law enforcement sensitive information relating to a requestor, which could possibly compromise ongoing criminal investigations if released to the requestor, pursuant to the Privacy Act. 5 U.S.C. 552a(k)(2).

Types of information sharing that may result from the routine uses outlined in this notice include: (1) Disclosure to individuals who are working as a contractor or with a similar relationship working on behalf of DHS; (2) sharing with Congressional offices asking on behalf of an individual; (3) sharing when there appears to be a specific violation or potential violation of law, or identified threat or potential threat to national or international security, such as criminal or terrorist activities, based on individual records in this system; (4) sharing with the National Archives and Records Administration (NARA) for proper handling of government records; (5) sharing when relevant to litigation associated with the Federal government; and (6) sharing to protect the individual who is the subject of the record from the harm of identity theft in the case of a data breach affecting this system.

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

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the Fraud Detection and National Security Data System 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–006.

SYSTEM NAME:

United States Citizenship and Immigration Services Fraud Detection and National Security Data System (FDNS–DS).

SECURITY CLASSIFICATION:

Sensitive But Unclassified.

SYSTEM LOCATION:

Records are maintained at the USCIS FDNS Headquarters in Washington, DC and field offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: Individuals covered by provisions of the Immigration and Nationality Act of the United States, 8 U.S.C. 1101 *et seq.,* including but not limited to applicants, beneficiaries, petitioners, and their authorized representatives (who may be U.S. citizens, lawful permanent residents, or aliens) submitting applications or petitions for immigration benefits. Individuals who are the subjects of administrative and/or criminal investigations, individuals who have submitted potentially fraudulent petitions and applications for immigration benefits, individuals whose petitions or applications have been randomly selected for assessment of the effectiveness of fraud detection programs (*i.e.,* BFAs), and individuals of concern based on possible national security reasons, public safety concerns or criminal activity. The system will contain information about organizations that may have submitted applications or petitions (*e.g.*, preparers, representatives, and petitioning organizations) on behalf of individuals and may contain information on individuals that are associated with an application but not actually applying for a benefit.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Individual's name;
- Alias;

- Social Security Number;
- A-Number;
- Associated A-Numbers of close relatives and associates;
- Receipt Number;
- Address (home and business);
- Date and place of birth;
- Country of citizenship;
- Citizenship status;
- Gender;
- Telephone number(s);
- E-mail address;
- Place of employment and employment history;
- Organizations (Place of business or place of worship, if place of worship is sponsoring the applicant);
- Family lineage;
- Bank account information and/or financial transaction history;
- Marriage record;
- Civil or criminal history information;
- Uniform resource locators (URLs);
- Education record;
- Internet protocol addresses;
- Biometric identifiers (Photographic facial image, fingerprints);
- TECS, NCIC, and data and analysis resulting from the investigation or routine background checks performed as part of the adjudication process;
- any other unique identifying number or characteristic.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Purpose(s):

The purpose of this system is to increase the effectiveness of the U.S. immigration system in identifying threats to national security, combating benefit fraud, and locating and removing vulnerabilities that compromise the integrity of the legal immigration system.

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 U.S. Attorneys' offices) 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. USCIS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. USCIS 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 that relies upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USCIS'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, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

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 disks that are backed up to disk and tape media.

RETRIEVABILITY:

Records may be retrieved by utilizing multiple data points that include an individual's last name, A-Number, 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. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary by component and program.

RETENTION AND DISPOSAL:

The National Archives Records Administration has not approved a retention schedule for this system of records. USCIS has proposed 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–DS. The 15-year retention schedule is proposed to provide 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 retention period, which is currently 75 years.

SYSTEM MANAGER AND ADDRESS:

Chief Information Officer, United States Citizenship and Immigration Services, 111 Massachusetts Avenue, NW., 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 the component's FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' 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–0550, 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 to you under 28 U.S.C. 1746, a law that permits statements to be made under penalty or 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,
- 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,
- 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 the component(s) will 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, and from members of the general public.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

Dated: August 11, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–19032 Filed 8–15–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Federal Emergency Management Agency

[FEMA–1768–DR]

Wisconsin; Amendment No. 15 to Notice of a Major Disaster Declaration

AGENCY: Federal Emergency Management Agency, DHS.

ACTION: Notice.

SUMMARY: This notice amends the notice of a major disaster declaration for the State of Wisconsin (FEMA–1768–DR), dated June 14, 2008, and related determinations.

DATES: *Effective Date:* August 8, 2008.

FOR FURTHER INFORMATION CONTACT: Peggy Miller, Disaster Assistance Directorate, Federal Emergency Management Agency, 500 C Street, SW., Washington, DC 20472, (202) 646–3886.

SUPPLEMENTARY INFORMATION: Notice is hereby given that pursuant to the President's June 30, 2008, amended declaration authorizing Federal funds for emergency protective measures, including direct Federal assistance, at 90 percent Federal funding of total eligible costs under the Public Assistance program, the National Oceanic and Atmospheric Administration's National Weather Service River Forecast Center has established that the rivers in the State of Wisconsin, which have experienced historical flooding, fell below flood stage on July 26, 2008.

(The following Catalog of Federal Domestic Assistance Numbers (CFDA) are to be used for reporting and drawing funds: 97.030, Community Disaster Loans; 97.031, Cora Brown Fund; 97.032, Crisis Counseling; 97.033, Disaster Legal Services; 97.034, Disaster Unemployment Assistance (DUA); 97.046, Fire Management Assistance Grant; 97.048, Disaster Housing Assistance to Individuals and Households In Presidentially Declared Disaster Areas; 97.049, Presidentially Declared Disaster Assistance—Disaster Housing Operations for Individuals and Households; 97.050, Presidentially Declared Disaster Assistance to Individuals and Households—Other Needs; 97.036,