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 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,
- 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:

Individuals who have been subject to search or arrest; owners, claimants, and other interested parties of detained, seized and/or forfeited property; other Federal agencies, and State, tribal and local law enforcement agencies; confidential sources; and members of the public.

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), and (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: November 28, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29055 Filed 12–8–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0186]

Privacy Act of 1974; U.S. Immigration and Customs Enforcement-006 Intelligence Records System (IIRS) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new system of records titled the U.S. Immigration and Customs Enforcement (ICE) Intelligence Records System (IIRS). IIRS contains information generated or received by the ICE Office of Intelligence, or other offices within ICE that support the law enforcement intelligence mission, that is analyzed and disseminated to ICE executive management and operational units for law enforcement, intelligence, counterterrorism, and other homeland security purposes. IIRS also contains data maintained in the Office of Intelligence's Intelligence Fusion System (IFS), a software application and data repository that facilitates research and analysis of information from a variety of sources within and outside of DHS to support law enforcement activities and investigations of violations of U.S. laws, administration of immigration laws and other laws administered or enforced by DHS, and production of DHS law enforcement intelligence products. Additionally, a Privacy Impact Assessment for IFS will be posted on the Department's privacy Web site. (See *www.dhs.gov/privacy* and follow the link to ''Privacy Impact Assessments.'') Due to urgent homeland security and law enforcement mission needs, IFS is currently in operation. Recognizing that ICE is publishing a notice of system of records for an existing system, ICE will carefully consider public comments, apply appropriate revisions, and republish the IIRS notice of system of records within 180 days of receipt of comments. A proposed rulemaking is also published in this issue of the **Federal Register** in which the Department proposes to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: The established system of records will be effective January 8, 2009. Written comments must be submitted on or before January 8, 2009. A revised IIRS notice of system of records that addresses public comments, responds to OMB direction, and includes other ICE changes will be published not later than July 7, 2009 and will supersede this notice of system of records.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0186 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: Lyn M. Rahilly (202–514–1900), Privacy Officer, U.S. Immigration and Customs Enforcement, 425 I Street, NW., Washington, DC 20001, or 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 ICE Intelligence Records System (IIRS) system of records is owned by the ICE Office of Intelligence. It consists of information generated or received by the Office of Intelligence, or other offices within ICE that support the law enforcement intelligence mission, that is analyzed and disseminated to ICE executive management and operational units for law enforcement, intelligence, counterterrorism, and other homeland security purposes. Using various databases and tools, the Office of Intelligence produces formal law-enforcement intelligence reports that are the end-result of the intelligence process. These reports, the underlying data on which they are based, and the work papers used or created by the analysts and agents, are all included within the IIRS system of records.

As part of the intelligence process, ICE investigators and analysts must review large amounts of data to identify and understand relationships between individuals, entities, threats, and events to generate law-enforcement intelligence products that provide ICE operational units with actionable information for law enforcement purposes. If performed manually, this process can involve hours of analysis of voluminous data. To automate and expedite this process, the former Immigration and Naturalization Service created a software application and data repository that allowed for the efficient research and analysis of data from a variety of sources. That application is now called the Intelligence Fusion System (IFS) and is currently owned by the ICE Office of Intelligence.

IFS is specifically designed to make the intelligence research and analysis process more efficient by allowing searches of a broad range of data through a single interface. IFS can also identify links (relationships) between individuals or entities based on commonalities, such as identification numbers, addresses, or other information. These commonalities in and of themselves are not suspicious, but in the context of additional information they sometimes help DHS agents and analysts to identify potentially criminal activity and identify other suspicious activities. These commonalities can also form the basis for a DHS-generated intelligence product that may lead to further investigation or other appropriate follow-up action by ICE, DHS, or other Federal, State, or local agencies.

DHS personnel may access IFS only if they hold positions that involve the execution of law enforcement responsibilities, the administration of immigration and naturalization laws, or the production of DHS intelligence products. While IFS does increase the efficiency of data research and analysis, it does not allow DHS personnel to obtain any data they could not otherwise access in the course of their job responsibilities. IFS does not seek to predict future behavior or ''profile'' individuals, *i.e.*, look for individuals who meet a certain pattern of behavior that has been pre-determined to be suspect.

Individuals may request information about records pertaining to them stored in IIRS as outlined in the ''Notification Procedure'' section below. ICE reserves the right to exempt various records from release pursuant to exemptions 5 U.S.C. 552a(j)(2) and (k)(2) of the Privacy Act.

Consistent with DHS's information sharing mission, information stored in IIRS 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 recordkeeping 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 IIRS 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/ICE–006

SYSTEM NAME:

ICE Intelligence Records System (IIRS).

SECURITY CLASSIFICATION:

Sensitive But Unclassified, Classified.

SYSTEM LOCATION:

Records are maintained at ICE Headquarters in Washington, DC, and field offices.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include the following: (1) Individuals (*e.g.*, subjects, witnesses, associates) associated with immigration enforcement activities or law enforcement investigations/activities conducted by ICE, the former Immigration and Naturalization Service, or the former U.S. Customs Service; (2) individuals associated with law enforcement investigations or activities conducted by other Federal, State, tribal, territorial, local or foreign agencies where there is a potential nexus to ICE's law enforcement and immigration enforcement responsibilities or homeland security in general; (3) individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism; (4) individuals involved in, associated with, or who have reported suspicious activities, threats, or other incidents reported by domestic and foreign government agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, and individuals; and (5) individuals who are the subjects of or otherwise identified in classified or unclassified intelligence reporting received or reviewed by ICE.

IIRS includes an information technology system known as the Intelligence Fusion System (IFS). In addition to the categories of individuals listed above, IFS also includes the following: (1) Individuals identified in law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies; (2) individuals identified in U.S. visa, border, immigration and naturalization benefit data, including arrival and departure data; (3) individuals identified in DHS law enforcement and immigration records; (4) individuals not authorized to work in the United States; (5) individuals whose passports have been lost or stolen; and (6) individuals identified in public news reports.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include: (1) Biographic information (name, date of birth, social security number, alien registration number, citizenship/immigration status, passport information, addresses, phone numbers, etc.); (2) Records of immigration enforcement activities or law enforcement investigations/activities conducted by ICE, the former Immigration and Naturalization Service, or the former U.S. Customs Service; (3) Information (including documents and electronic data) collected by DHS from or about individuals during investigative activities and border searches; (4) Records of immigration enforcement activities and law enforcement investigations/activities that have a possible nexus to ICE's law enforcement and immigration enforcement responsibilities or homeland security in general; (5) Law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies; (6) U.S. visa, border immigration and naturalization benefit data, including arrival and departure data; (7) Terrorist watchlist information and other terrorism related information regarding threats, activities, and incidents; (8) Lost and stolen passport data; (9) Records pertaining to known or suspected terrorists, terrorist incidents, activities, groups, and threats; (10) ICE-generated intelligence requirements, analysis, reporting, and briefings; (11) Third party intelligence reporting; (12) Articles, public-source data, and other published information on individuals and events of interest to ICE; (13) Records and information from government data systems or retrieved from commercial data providers in the course of intelligence research, analysis and reporting; and (14) Reports of suspicious activities, threats, or other incidents generated by ICE and third parties.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 8 U.S.C. 1103, 1105, 1225(d)(3), 1324(b)(3), 1357(a), and 1360(b); 19 U.S.C. 1 and 1509.

PURPOSE(S):

(a) To maintain records that reflect and generally support ICE's collection, analysis, reporting, and distribution of law enforcement, immigration administration, terrorism, intelligence, and homeland security information in support of ICE's law enforcement and immigration administration mission.

(b) To produce law-enforcement intelligence reporting that provides actionable information to ICE's law enforcement and immigration administration personnel and to other appropriate government agencies.

(c) To enhance the efficiency and effectiveness of the research and analysis process for DHS law enforcement, immigration, and intelligence personnel through information technology tools that provide for advanced search and analysis of various datasets; and

(d) To identify potential criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.

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 or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when (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 the Department of Justice (DOJ), Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction to include allegations of fraud and/or nationality discrimination.

C. 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.

D. 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.

E. 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.

F. 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) that rely upon the compromised information, or harm to an individual; 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.

G. 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.

H. To a Federal, State, territorial, tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the

operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

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

J. To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to the agency's decision concerning the hiring or retention of an individual or the issuance, grant, renewal, suspension or revocation 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 receiving the information.

K. 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, including 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 risk.

L. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

M. To a Federal, State, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

N. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil, criminal, or regulatory laws.

O. To third parties during the course of an investigation by DHS, a proceeding within the purview of the immigration and nationality laws, or a matter under DHS's jurisdiction, 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.

P. To a Federal, State, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

Q. To Federal and foreign government intelligence or counterterrorism agencies when DHS 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.

R. To an organization or individual in either the public or private sector, either foreign or domestic, where 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 and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

S. To international and foreign governmental authorities in accordance with law and formal or informal international agreements.

T. 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.

U. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations where DHS is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance national security or identify other violations of law.

V. To appropriate Federal, State, local, tribal, or foreign government agencies or multinational government organizations where DHS desires to exchange relevant data for the purpose of developing new software or implementing new technologies for the purposes of data sharing to enhance homeland security, national security or law enforcement.

W. 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 personal identifiers such as but not limited to name, alien registration number, phone number, address, social security number, or passport number. Records may also be retrieved by non-personal information such as transaction date, entity/institution name, description of goods, value of transactions, and other information.

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:

ICE is in the process of drafting a proposed record retention schedule for the information maintained in IIRS, including system information stored in IFS. ICE anticipates retaining the records from other databases in IFS for 20 years, records for which IFS is the repository of record for 75 years, and ICE-generated intelligence reports for 75 years. The original electronic data containing the inputs to IFS will be destroyed after upload and verification or returned to the source.

SYSTEM MANAGER AND ADDRESS:

Director, ICE Office of Intelligence, 425 I Street NW., Washington DC 20536.

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 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:

Federal, State, local, territorial, tribal or other domestic agencies, foreign agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, individuals, commercial data providers, and public sources such as news media outlets and the Internet.

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).

Dated: December 1, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29056 Filed 12–8–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0132]

Privacy Act of 1974; Immigration and Customs Enforcement (ICE)–007 Law Enforcement Support Center (LESC) Alien Criminal Response Information Management (ACRIMe) 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 (DHS) is giving notice that it proposes to update and reissue the following legacy record system Justice/INS. 023 Law Enforcement Support Center Database as an Immigration and Customs Enforcement (ICE) system of records titled Law Enforcement Support Center (LESC) Alien Criminal Response Information Management System (ACRIMe). The information in this system of records includes data collected and maintained by the ICE LESC to carry out its mission to respond to inquiries from law enforcement agencies concerning immigration status of an individual, and whether the individual is under investigation and/or wanted by ICE or other law enforcement agencies. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have been updated. Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the **Federal Register**. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been completed. This system will be included in the DHS inventory of record systems.

DATES: Written comments must be submitted on or before January 8, 2009. This new system will be effective January 8, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0132 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