Periodically, CDC estimates the overall burden of foodborne illness. CDC's estimate of the overall burden of foodborne illness has a much larger scope than CDC's annual reports and draws heavily from FoodNet data as well as from a much wider variety of data sources, both inside and outside of CDC. This estimate also includes norovirus, a major contributor to the overall burden of foodborne disease, which can be transmitted not only by foods, but also by environmental sources, and is not monitored by FoodNet. CDC's last estimate of the overall burden of foodborne illness was issued in 1999 and included unknown causes of foodborne illness (Ref. 2). Since then, advances in methodology and data sources have improved capabilities in developing disease burden estimates; these will be reflected in CDC's next estimate.

In addition to CDC estimates, FDA and USDA use other measures to gauge the success, or implied success (i.e., via proxy measures), of policies and interventions for reducing foodborne illness. For example, although measurements of the food industry's compliance with a given food safety regulation cannot be used to directly measure the regulation's impact on the rate of foodborne illness, improved compliance can be reasonably expected to improve the likelihood that the foods involved will be safer and, thus, the likelihood that fewer illnesses will result. Examples include the tracking of *E. coli* O157:H7 in ground beef and of *Salmonella* in meat, and surveys of both domestic and imported produce, such as surveys conducted by FDA and USDA's Microbiological Data Program, which have targeted *Salmonella* and *E. coli* O157:H7.

II. Purpose of the Workshop and Topics for Discussion

The purpose of this initial 1-day public workshop is to discuss current and potential measurements for assessing progress in food safety and to provide workshop participants an opportunity to learn about metrics and to consider and suggest metrics for assessing the effects that policies and interventions have on foodborne illness. The workshop will focus on the current status and challenges involved in measuring foodborne illness and trends over time, including incidence and trends in the overall burden of foodborne illness and illnesses associated with specific foodborne pathogens and specific pathogens that affect specific foods. The workshop will include a discussion of other measures that are, or could be, used to measure food safety progress that cannot be directly linked to health outcomes. These include measures of process control in food production, studies on the prevalence of specific pathogens in specific classes of food, and studies of compliance with recommended or required food safety practices in retail and food-service operations.

Specifically, topics to be discussed include CDC's data sources and methods, including methods for estimating the burden of foodborne illness, and their various limitations and utilities; and FDA's and USDA's ongoing measures to gauge the success, or implied success (i.e., via the kinds of proxy measures described in previously mentioned examples; e.g., surveys for *E. coli* O157:H7 and *Salmonella* in produce and tracking of specific pathogens in meat), of policies and interventions, including the level of compliance with food safety regulations.

III. Transcripts

Please be advised that as soon as a transcript is available, it will be accessible at *http://www.regulations.gov*. It may be viewed at the Division of Dockets Management (HFA–305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. A transcript will also be available in either hardcopy or on CD–ROM, after submission of a Freedom of Information request. Written requests are to be sent to Division of Freedom of Information (HFI–35), Office of Management Programs, Food and Drug Administration, 5600 Fishers Lane, rm. 6–30, Rockville, MD 20857.

IV. References

The following references are on display at the Division of Dockets Management (see *Transcripts*), between 9 a.m. and 4 p.m., Monday through Friday. (FDA has verified the following Web site address, but FDA is not responsible for any subsequent changes to the Web site after this document publishes in the **Federal Register**.)

1. President's Food Safety Working Group findings, *http://www.foodsafetyworkinggroup.gov/ContentKeyFindings/HomeKeyFindings.htm*.

2. Mead P.S., L. Slutsker, V. Dietz, et al., *Food-Related Illness and Death in the United States*, *Emerging Infectious Diseases*, 5(5), 607–625, 1999.

Dated: February 23, 2010.

Leslie Kux,

Acting Assistant Commissioner for Policy.

[FR Doc. 2010–4110 Filed 2–26–10; 8:45 am]

BILLING CODE 4160–01–S

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0071]

Privacy Act of 1974; U.S. Immigration and Customs Enforcement–006 Intelligence Records System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, U.S. Immigration and Customs Enforcement is modifying an existing system of records titled the Immigration and Customs Enforcement–006 Intelligence Records System (Dec. 9, 2008), to clarify the nature of the personally identifiable information that will be collected and maintained on individuals. In conjunction with its publication of the Privacy Impact Assessment for the ICEGangs system, Immigration and Customs Enforcement is modifying the DHS/ICE–006 Immigration and Customs Enforcement Intelligence Records system of records notice to more clearly explain the type of information it gathers on suspected and confirmed gang members and associates. This DHS/Immigration and Customs Enforcement–006 Intelligence Records system of records notice updates categories of individuals; categories of records; purpose of the system; adding a routine use; and policies and practices for retaining and disposing of records in the system. Immigration and Customs Enforcement is soliciting comments on this SORN due to the clarifying changes that were made since the original publication. A Privacy Impact Assessment on ICEGangs that describes the system in detail is being published concurrently with this notice. In addition, this notice addresses one comment that was received in response to the original publication of the Immigration and Customs Enforcement Intelligence Records SORN on December 9, 2008. A final rule is being published concurrently with this notice in which the Department exempts portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: This amended system of records will be effective March 31, 2010. Written comments must be submitted on or before March 31, 2010.

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

2009–0071 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *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 Lyn M. Rahilly (202–732–3300), Privacy Officer, U.S. Immigration and Customs Enforcement, 500 12th Street, SW., Washington, DC 20536. For privacy issues please contact Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

The Immigration and Customs Enforcement (ICE) Intelligence Records (IIRS) system of records was originally established on December 9, 2008 (73 FR 74735), and public comments were solicited for the SORN and the associated Notice of Proposed Rulemaking (73 FR 74633, Dec. 9, 2008) which proposed to exempt this system from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. Due to urgent homeland security and law enforcement mission needs, ICE was already maintaining these records when the original IIRS SORN was published. Recognizing that ICE published a system of records notice for an existing system, ICE committed to reviewing and considering public comments, apply appropriate revisions, and republish the IIRS system of records notice within 180 days of receipt of comments. A new routine use is also proposed to allow data sharing between ICE and other law enforcement agencies for the purpose of collaboration, coordination, and de-confliction of cases.

In addition to the records described in the initial publication of IIRS, this notice also consists of information maintained by the ICE Office of Investigations concerning suspected or confirmed gang members and associates included in a database called ICEGangs. ICEGangs maintains personal information about individuals who qualify as suspected or confirmed gang members and associates under ICE criteria. ICEGangs stores the following data about each gang member and associate to the extent it is available: Biographic information (name, date of birth, *etc.*), immigration status, gang affiliation, physical description, government-issued identification numbers, photos of the individual, identities of gang associates, field interview notes, and criminal history information. ICEGangs also stores general comments entered by the ICE agent that created the gang member or associate record as well as a reference to the official evidentiary system of records where official case files are stored.

ICEGangs has two main purposes. First, it supplements the existing ICE case management system by providing a consolidated repository of information on gang members and associates and gang-related activity. ICEGangs allows ICE agents and support personnel to search gang-oriented information in a more efficient and effective manner than is possible in ICE's standard investigative case management system. For example, an ICE field agent can query ICEGangs for a list of members in a specific gang. It is not currently possible to perform the same sort of query using ICE's investigative case management system. As a matter of policy, ICE agents are required to create and/or update ICEGangs records for suspected and/or confirmed gang members and associates whenever they encounter gang members and associates in the field during their official law enforcement activities. ICEGangs records also contain references to the official evidentiary system of records, which allows ICE agents and support personnel to refer to official case records.

Second, ICEGangs facilitates the sharing of gang information between ICE and other law enforcement agencies. In particular, ICE currently provides the California Department of Justice (CalDOJ) access to the data in ICEGangs. CalDOJ users access ICEGangs through their own CalGangs application which accesses the ICEGangs repository remotely. In the future, ICE anticipates that it will share information with other State and local law enforcement agencies that use the GangNET software. ICE will require access controls for State and local agencies as a prerequisite to gaining access to ICEGangs.

II. Public Comment

One public comment was received, but as it did not pertain to the SORN or proposed rule, it is not addressed here. A final rule is published concurrently with this notice in this issue of the **Federal Register**.

III. 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 Immigration and Customs Enforcement–006 Intelligence Records 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; (5) individuals who are the subjects of or otherwise identified in classified or unclassified intelligence reporting received or reviewed by ICE; and (6) individuals who are known or suspected gang members or associates, including records maintained in the ICEGangs system.

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; (14) Reports of suspicious activities, threats, or other incidents generated by ICE and third parties; and (15) Additional information about known and suspected gang members and associates such as biographic information (name, date of birth, *etc.*), immigration status, gang affiliation, physical description, government-issued identification numbers, photos of the individual, identities of gang associates, field interview notes, and criminal history information.

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):

The purpose of this system is:

(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.

(d) To facilitate multi-jurisdictional informational exchange between ICE and other law enforcement agencies regarding known and suspected gang members and associates; and

(e) 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 a criminal, civil, or regulatory law enforcement authority (whether Federal, State, local, territorial, Tribal, international or foreign) where the information is necessary for collaboration, coordination and de-confliction of investigative matters, to avoid duplicative or disruptive efforts and for the safety of law enforcement officers who may be working on related investigations.

X. 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.

ICE is in the process of drafting a proposed record retention schedule for the information maintained in ICEGangs. ICE anticipates retaining ICEGangs records for five years from the date the record was last accessed.

SYSTEM MANAGER AND ADDRESS:

Director, ICE Office of Intelligence, 500 12th Street, SW., Washington, DC 20536.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, ICE will consider individual requests to determine whether or not information may be released. Thus, 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 form 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: February 24, 2010.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2010–4102 Filed 2–26–10; 8:45 am]

BILLING CODE 9111–28–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0144]

Privacy Act of 1974; Department of Homeland Security United States Immigration Customs and Enforcement—011 Immigration and Enforcement Operational Records System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of amendment of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974 the Department of Homeland Security U.S. Immigration and Customs Enforcement is updating an existing system of records titled, Department of Homeland Security/U.S. Immigration and Customs Enforcement—011 Removable Alien Records System of Records, January 28, 2009, and renaming it Department of Homeland Security/U.S. Immigration and Customs Enforcement—011 Immigration and Enforcement Operational Records System of Records. With the publication of this updated system of records, the Department of Homeland Security is also retiring an existing system of records titled, Department of Homeland Security/U.S. Immigration and Customs Enforcement—Customs and Border Protection—U.S. Citizenship and Immigration Services—001–03 Enforcement Operational Immigration Records System of Records, March 20, 2006, and transferring certain law enforcement and immigration records described therein that are owned by U.S. Immigration and Customs Enforcement to this updated system of records. Categories of individuals and categories of records have been reviewed, and the purpose statement and routine uses of this system have been updated to better reflect the current status of these records. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This updated system will continue to be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before March 31, 2010. This amended system will be effective March 31, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS–2009–0144 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *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: Lyn Rahilly (703–732–3300), Privacy Officer, U.S. Immigration and Customs Enforcement, 500 12th Street, SW., Washington, DC 20536; or Mary Ellen Callahan (703–235–0780), 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, the Department of Homeland Security is updating and reissuing Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE)—011 Removable Alien Records System of Records (74 FR 4965, Jan. 28, 2009) to include additional DHS records pertaining to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by DHS. This system of records is also being updated to include records pertaining to fugitive aliens and aliens paroled into the United States (U.S.) by ICE. The system of records is being renamed DHS/ICE–011 Immigration and Enforcement Operational Records System of Records (ENFORCE) to better reflect the nature and scope of the records maintained.

DHS is updating this notice to include the following substantive changes: (1) An update to the categories of records to include clarifying language as well as to provide the Department of Justice (DOJ) with DNA samples as required by 28 CFR Part 28; (2) the addition of routine uses to (a) incorporate the routine uses that were already part of the published DHS/ICE—011 Removable Aliens Records System of Records (RARS) (74 FR 20719, May 5, 2009) into this newly consolidated SORN, (b) provide information to individuals in the determination of whether or not an alien has been removed from the U.S., (c) assist agencies in collecting debts owed to them or the U.S. Government, (d) allow sharing with the Department of State (DOS) for immigration benefits and visa activities, as well as when DOS is contacted by foreign governments to discuss particular matters involving aliens in custody or other ICE enforcement matters that may involve identified individuals, (e) allow the Office of Management and Budget (OMB) to review the private immigration relief bill process in Congress, (f) inform members of Congress about an alien who is being considered for private immigration relief, (g) share operational information with other law enforcement agencies to prevent conflicting investigations or activities, (h) coordinate the transportation, custody, and care of U.S. Marshals Service (USMS) prisoners, (i) allow third parties to facilitate the placement or release of an alien who has been or are in the process of being released from ICE custody, (j) provide information about an alien who has or is in the process of being released from ICE custody who may pose a health or safety risk, (k) to provide information facilitating the issuance of an immigration detainer on an individual in custody or the transfer of an individual to ICE or another agency, (l) disclose DNA samples and related information as required by Federal regulation, (m) to facilitate the transmission of arrest information to the Department of Justice for inclusion in relevant law enforcement databases and for the enforcement Federal firearms licensing laws, and (n) to disclose information to persons seeking to post or arrange immigration bonds. These updated routine uses are compatible with the purpose of this system because