



## DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2012-0069]

Privacy Act of 1974; Department of Homeland Security Immigration and Customs Enforcement-007 – Alien Criminal Response Information Management System of Records

**AGENCY:** Department of Homeland Security, Privacy Office.

**ACTION:** Notice of modification to existing 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 and renaming an existing system of records titled, “Department of Homeland Security/Immigration and Customs Enforcement-007 – Law Enforcement Support Center Alien Criminal Response Information Management System of Records.” With the publication of this updated system of records, several changes are being made: 1) the name is being changed; 2) new categories of individuals have been added; 3) new routine uses have been added to allow Immigration and Customs Enforcement to share information from the system; and 4) the retention period of Brady Act check records has been corrected and the retention period for National Sex Offender Registrant records and for individuals for whom non-criminal queries are conducted have been added. A Privacy Impact Assessment update for the Alien Criminal Response Information Management system is being published concurrently with this notice. It can be found on the DHS website at <http://www.dhs.gov/privacy>. The exemptions for the existing system of records notice

will continue to be applicable for this system of records notice (74 FR 45079, August 31, 2009), and this system will continue to be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. In particular, comments are requested concerning the application of the exemptions to the newly added categories of individuals. This new system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit comments, identified by docket number DHS-2012-0069 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 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 (202-732-3300), Privacy Officer, U.S. Immigration and Customs Enforcement, 500 12th Street, S.W., Stop 5004 Washington, D.C. 20536-5004; Jonathan R. Cantor, (202-343-1717), Acting Chief

Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

**SUPPLEMENTARY INFORMATION:**

I. Background

The Department of Homeland Security (DHS) is updating and reissuing DHS/ Immigration and Customs Enforcement (ICE)-007 – Law Enforcement Support Center (LESC) Alien Criminal Response Information Management System (ACRIME) system of records notice (SORN) (75 FR 8377, February 24, 2010), to shorten the system name, add new categories of individuals and routine uses, and update the retention period of records related to Brady Act checks, National Sex Offender Registrants, and individuals for whom non-criminal queries are conducted. The new system name is DHS/ICE-007 – Alien Criminal Response Information Management System (ACRIME). This system of records describes information maintained in an ICE information system of the same name, which is used by ICE personnel to receive and respond to immigration status inquiries made by other agencies about individuals who are arrested, screened as part of a background check in order to determine suitability for employment, access, or other purposes, or otherwise encountered by those agencies. ACRIME also supports the creation and maintenance of lookout records in the Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC) system on persons wanted by ICE for crimes or as fugitive aliens. ACRIME also supports the operation of the ICE tip line, where members of the public can notify ICE of suspected violations of law, and the operation of the Law Enforcement Support Center call center, which takes calls from other law enforcement agencies seeking assistance from ICE.

Concurrent with the publication of this SORN update, ICE is publishing an update to the ACRIME Privacy Impact Assessment (PIA) to describe several updates to the data maintained in that system in support of ICE's immigration enforcement mission. ICE is adding new categories of individuals to the DHS/ICE-007 – ACRIME SORN to adequately describe the individuals whose information is maintained in the system via the interoperability process. The ACRIME PIA update is available on the DHS Privacy Office web site at <http://www.dhs.gov/privacy>.

Under interoperability's original use, the fingerprints of individuals arrested by or in the custody of a law enforcement agency participating in the ICE Secure Communities Program are sent to the FBI's Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) for matching against the FBI's criminal fingerprint holdings. Through interoperability, the fingerprints are also checked against the DHS Automated Biometric Identification System (IDENT) and, if the submitted fingerprints match fingerprints in IDENT, the FBI generates an Immigration Alien Query (IAQ) that is sent to the ACRIME. An ICE employee uses ACRIME to research the subject of the IAQ, determine the immigration status of the subject, and generate an Immigration Alien Response (IAR), which ACRIME sends back to the FBI Criminal Justice Information Services (CJIS) Division. The FBI combines and sends the IDENT response and the IAR back to the agency that conducted the fingerprint check for awareness if they are technically capable of receiving the response. ACRIME also sends the IAR to the appropriate ICE field office to determine the appropriate enforcement action, if any, to take against the individual.

As described in the ACRIME PIA update, ACRIME's use under interoperability has been expanded to assist other agencies that screen individuals for various purposes, including administration of criminal justice, national security, and background checks/investigations conducted for employment, access, and other suitability purposes. The appendices to the PIA list the new uses of interoperability that ACRIME now supports. The appendices will be updated as new interoperability users are added and as existing users change how they use interoperability. It should be noted that although ACRIME is supporting new uses under interoperability, the process by which IAQs (queries) are submitted to ACRIME and responses (IARs) are sent back to the FBI CJIS Division and ultimately to the agency submitting the request, remains the same as occurs under Secure Communities. For example, one of the new uses of ACRIME is to assist agencies that are conducting background checks/investigations on individuals for employment, access, or other suitability purposes. The fingerprints of the individuals being screened are checked against IDENT and IAQs are sent to ACRIME for any matches. ICE personnel research the subjects of the IAQ, determine the immigration status of the subjects, and return IARs on them.

Using interoperability, ICE will also begin to screen convicted sex offenders whose fingerprints are captured during federal, state, local, and tribal law enforcement processes that enroll these individuals in sex offender registries. ICE places a high priority on targeting for removal those aliens with criminal records who pose a threat to public safety, such as sex offenders. When a convicted sex offender is released from incarceration, the individual is required to register as a sex offender with authorities in the state in which he or she resides. During the registration process, state authorities

typically capture the individual's fingerprints and biographic information and transmit them to the FBI CJIS Division for inclusion in the National Sex Offender Registry, and to update IAFIS and the individual's FBI criminal record. Via interoperability, the FBI CJIS Division automatically runs the individual's fingerprints against IDENT. If the fingerprints match fingerprints in IDENT, an IAQ is generated and sent to ACRIME. ICE users research the immigration status of the individual and generate an IAR containing the results of that research in ACRIME. The IAR is sent to the relevant ICE field office, which determines the appropriate enforcement action to take against the individual, if any. A similar process is used when there are changes to the convicted sex offender's information. The state authorities send the individual's information to the FBI CJIS Division. They update the person's record, run the individual's fingerprints against IDENT, and if the fingerprints match fingerprints in IDENT, an IAQ is generated and sent to ACRIME. The processing of the convicted sex offender information varies from the standard interoperability process in one respect only: ACRIME does not send a copy of the IAR to the FBI CJIS Division or to the agency that registered the sex offender. Instead, the IAR is only distributed and used within ICE for enforcement purposes.

New categories of individuals have been added to the DHS/ICE-007 – ACRIME SORN to describe the convicted sex offenders and other types of individuals whose information is being processed through ACRIME under these new interoperability programs including individuals about whom a background check is being performed for employment, access, or other suitability purposes. As new interoperability users are approved by DHS, the ACRIME PIA appendix will be updated to describe them and conforming changes will be made to this SORN, if required.

Additionally, new routine uses have been added to allow ICE to share information from the system. Below is a summary of the new routine uses and their corresponding letter:

(J) To federal, state, local, tribal, territorial, or international agencies seeking to verify or ascertain the citizenship or immigration status of an individual for a purpose within the agency's jurisdiction;

(N) To a former employee of DHS for purposes of responding to an official inquiry or facilitating communications with a former employee that may be relevant for personnel-related or other official purposes;

(V) To prospective claimants and their attorneys for the purpose of negotiating the settlement of an actual or prospective claim against DHS prior to litigation or proceedings;

(X) To the Department of Justice (DOJ), Federal Bureau of Investigation (FBI) in order to facilitate responses to fingerprint-based immigration status queries;

(Y) To federal, state, local, tribal, territorial, international, or foreign government agencies or entities to enable consultation to assist in the processing of redress requests;

(Z) To federal, state, local, tribal, territorial, foreign, or international agencies regarding a requesting agency's decision concerning the hiring or retention of an individual or if the information is relevant and necessary to a DHS decision concerning the hiring or retention;

(AA) To federal, state, local, tribal, territorial, foreign, or international agencies, if DHS determines the information is relevant and necessary to the agency's decision

concerning the hiring or retention of an individual and failure to disclose the information is likely to create a risk;

(BB) To federal, state, local, tribal, territorial, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts for law enforcement purposes;

(CC) To federal, state, local, tribal, territorial, or foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence;

(DD) To foreign governments in order to notify them concerning an alien who is incapacitated, an unaccompanied minor, or deceased.

(EE) To federal, state, local, tribal, and territorial courts or government agencies involved in criminal investigation or prosecution, pretrial services, sentencing, parole, probation or other aspects of the criminal justice process, and to counsel representing an individual in a proceeding, in order to ensure the integrity of the justice system by informing these recipients of the existence of an immigration detainer on that individual or that individual's status in removal proceedings, voluntary departure, or custodial status/location.

Finally, the retention period for Brady Act check records has been corrected. Previously, the SORN incorrectly stated that the records were retained for twenty-four (24) hours. The records are retained for five (5) years in order to provide ICE with sufficient time to follow up on any leads generated by Brady Act record check information. Additionally, the SORN is being updated to reflect the retention period for biometric and biographic immigration status check records for National Sex Offender

Registrants and individuals for whom non-criminal queries are conducted. Information on National Sex Offender Registrants will be maintained for seventy-five (75) years while records pertaining to non-criminal queries will only be retained for thirty (30) years.

Portions of the DHS/ICE-007 ACRIME System of Records are exempt from one or more provisions of the Privacy Act because of criminal, civil and administrative enforcement requirements. Individuals may request information about records pertaining to them stored in the DHS/ICE-007 ACRIME System of Records as outlined in the “Notification Procedure” section below. ICE reserves the right to exempt various records from release. Pursuant to 5 U.S.C. § 552a(j)(2), the Secretary of Homeland Security has exempted portions of this system of records from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (4)(H), (5) and (8); (f); and (g) of the Privacy Act. In addition, the system has been exempted from subsections (c)(3) and (4); (d); (e)(1), (4)(G), (4)(H), and (f) pursuant to 5 U.S.C. § 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. § 553(b), (c), and (e) and have been published in the Federal Register as addition to Title 28, Code of Federal Regulations (28 C.F.R. § 16.99). 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. In the context of this updated SORN, the Department is requesting comment on the application of these exemptions to the newly added categories of individuals.

## II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses,

and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other particular identifier assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when 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 their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/ICE-007 ACRIME System of Records.

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

**System of Records**

DHS/ICE – 007

**System name:**

Alien Criminal Response Information Management (ACRIME)

**Security classification:**

Unclassified and Law Enforcement Sensitive (LES).

**System location:**

Records are maintained in the ACRIME information technology system and associated paper records at the U.S. Immigration and Customs Enforcement (ICE) Law Enforcement Support Center (LESC) in Williston, Vermont, at ICE Headquarters, and at other ICE field office locations.

**Categories of individuals covered by the system:**

Categories of individuals covered in this system include:

(1) Individuals who are the subjects of immigration status inquiries submitted to

ICE or immigration checks conducted by ICE, including:

- A. Individuals who are encountered by, arrested by, under the investigation of, or in the custody of a criminal justice agency.
- B. Individuals convicted of sexual offenses required to register as a sexual offender.
- C. Individuals subject to background checks or investigations by or under the authority of a federal, state, local, tribal, or territorial agency to determine eligibility or suitability for employment, access, or other purposes.
- D. Individuals applying to obtain/purchase a firearm in the United States and whose information has been submitted to ICE for the purpose of conducting an immigration status check in support of background checks required by the Brady Handgun Violence

Protection Act (Brady Act) or other applicable laws.

- (2) Individuals who are the subjects of criminal arrest warrants and immigration lookouts that ICE has entered into the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) System.
- (3) Individuals who report tips concerning customs and immigration violations, suspicious activity or other law enforcement matters to the Department of Homeland Security (DHS)/ICE and individuals about whom those reports are made.
- (4) Law enforcement officers or other personnel working for criminal justice agencies who contact ICE for reasons relating to the purposes of this system of records, or for other law enforcement assistance.

**Categories of records in the system:**

Categories of records in this system may include:

- (1) Biographic identifiers, other identifiers, and contact information (e.g., name, aliases, date and place of birth, address, telephone number, Social Security Number (SSN), Alien Registration Number (A-Number), driver's license number, other personal identification numbers, fingerprint identification number, passport number).
- (2) Visa, border, immigration and citizenship information (e.g., citizenship and/or immigration status, application for benefit information, visa and travel history).
- (3) Criminal history information (e.g., FBI number, booking number, current charge[s], custodial status, past offenses and convictions).

- (4) NCIC hit confirmation records, which consist of information supporting the entry of criminal warrants or immigration lookouts into the NCIC system, such as criminal arrest warrant information, fingerprints and photographs, other information identifying the individual, and records reflecting the purpose/basis for the warrant or lookout. Records of inquiries received from criminal justice agencies regarding potential matches against ICE-created NCIC records, and records pertaining to ICE's research, resolution, and response to those inquiries.
- (5) Background investigation records, which consist of identifying and other information received from agencies requesting an immigration status check on individuals as part of a background check for employment, gun ownership, or other reasons; research conducted by ICE during the conduct of the immigration status check; and ICE's research, resolution, and response to those inquiries.
- (6) Criminal justice immigration status check records, which consist of identifying and other information received from criminal justice agencies requesting an immigration status check on individuals in the context of a criminal justice matter; prioritization of requests; research conducted by ICE during the conduct of the immigration status check; and ICE's research, resolution, and response to those inquiries.
- (7) Public tip records, which consist of information contained in tips received from the public or other sources regarding customs and immigration violations, or other violations of law, and suspicious activities. This includes

identifying and contact information about the individual reporting the tip (if provided) and information about the person or persons who are the subject of the tip.

- (8) Information pertaining to ICE's follow-up activities regarding a tip or other information received pursuant to the activities supported by this system of records, including leads for ICE investigations and referrals to other agencies.
- (9) Identification and authentication information for law enforcement officers or other criminal justice personnel who contact ICE.

**Authority for maintenance of the system:** 8 U.S.C. § 1103, 8 U.S.C § 1324(b)(3); 8 U.S.C § 1360(b); Section 504 of the Immigration and Nationality Act of 1990 (INA) (Pub. L. 101-649); the Brady Handgun Violence Protection Act of 1993 (Pub. L. 103-159); FY 2008 Consolidated Appropriations Act (Pub. L. 110-161, 121 Stat. 1844, 2050 (2007)); and the INA provisions regarding removal of criminal aliens (INA § 237(a)(2) and § 238).

**Purpose(s):**

The purposes of this system are to:

- (1) Identify and arrest individuals in the United States who may be subject to removal under the Immigration and Nationality Act, as amended.
- (2) Respond to inquiries from criminal justice agencies that seek to determine the immigration status of an individual in the context of a criminal justice matter for the purpose of identifying and arresting those who may be subject to removal.
- (3) Inform criminal justice agencies and agencies conducting background checks whether an individual is under investigation and/or wanted by ICE or other criminal

justice agencies.

(4) Receive, process and act on information received from the general public and other sources regarding suspicious activities and actual or potential violations of laws enforced by ICE or DHS, and to refer any other actionable information to the appropriate agencies for action.

(5) Provide assistance to domestic, foreign, and international agencies that contact ICE and the LESC on matters within the scope of ICE's law enforcement authorities, including violations of U.S. customs and immigration laws.

(6) Collect and analyze data to evaluate the effectiveness and quality of services provided to other agencies in support of the purposes described above, and of ICE's customs and immigration law enforcement efforts generally.

(7) Identify potential criminal activity, immigration violations, and threats to homeland security; uphold and enforce the law; and 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 (DOJ), including U.S. Attorneys Offices, or other federal agency conducting litigation or proceedings before any court, adjudicative or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. Any employee of DHS in his/her official capacity;
3. Any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made pursuant to a written Privacy Act waiver at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, 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; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS' 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 federal, state, local, tribal, territorial, or foreign government agencies or multilateral government 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.

H. To federal, state, local, tribal, territorial, foreign, or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning individuals who are being screened with respect to their participation in, attendance at, or other relation to a national or special security event.

I. To domestic governmental agencies seeking to determine the immigration status of persons who have applied to purchase/obtain a firearm in the United States, pursuant to checks conducted on such persons under the Brady Handgun Violence Prevention Act or other applicable laws.

J. To federal, state, local, tribal, territorial, or international agencies seeking to verify or ascertain the citizenship or immigration status of any individual within the jurisdiction of the agency for any purpose authorized by law.

K. To courts, magistrates, administrative tribunals, opposing counsel, parties, and witnesses, in the course of immigration, civil, or criminal proceedings (including discovery, presentation of evidence, and settlement negotiations) and when DHS determines that use of such records is relevant and necessary to the litigation before a court or adjudicative body when any of the following is a party to or have an interest in the 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 the government has agreed to represent the employee; or
4. The United States, where DHS determines that litigation is likely to affect DHS or any of its components.

L. To federal, state, local, tribal, territorial, foreign or international agencies in order to refer reports of suspicious activity, tips, potential violations of law and other relevant information to agencies with appropriate jurisdiction, authorities, and/or need-to-know concerning the matters.

M. To the Department of Justice (DOJ), Federal Bureau of Prisons (BOP) and other federal, state, local, territorial, tribal and foreign law enforcement or custodial agencies for the purpose of placing an immigration detainer on an individual in that

agency's custody, or to facilitate the transfer of custody of an individual to DHS from the other agency.

N. To a former employee of DHS for purposes of responding to an official inquiry by federal, state, local, tribal, territorial government agencies or professional licensing authorities; or facilitating communications with a former employee that may be relevant and necessary for personnel-related or other official purposes where DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

O. To federal, state, local, tribal, territorial, or foreign government agencies, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates or to elicit information required by DHS to carry out its functions and statutory mandates.

P. To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

Q. To the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in the Circular.

R. To the U.S. Senate Committee on the Judiciary or the U.S. House of Representatives Committee on the Judiciary when necessary to inform members of Congress about an alien who is being considered for private immigration relief.

S. To the Department of State when it requires information to consider and/or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about an alien or an enforcement operation with transnational implications.

T. To federal, state, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authorities when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, and/or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

U. To federal, state, local, tribal, territorial, or foreign government agencies or entities or multinational government agencies where DHS desires to exchange relevant data for the purpose of developing, testing, or implementing new software or technology whose purpose is related to this system of records.

V. To prospective claimants and their attorneys for the purpose of negotiating the settlement of an actual or prospective claim against DHS or its current or former employees, in advance of the initiation of formal litigation or proceedings.

W. To federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such disclosure is to support the conduct of national intelligence and security investigations or to assist in anti-terrorism efforts.

X. To the Department of Justice (DOJ), Federal Bureau of Investigation (FBI) in order to facilitate responses to fingerprint-based immigration status queries that are sent to ICE, including queries that the FBI sends on behalf of another agency.

Y. To federal, state, local, tribal, territorial, international, or foreign government agencies or entities 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. To verify the identity of an individual seeking redress in connection with the operations of a DHS component or program; or

3. To verify the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

Z. To federal, state, local, tribal, territorial, foreign, or international agencies, if the information is relevant and necessary to a requesting 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.

AA. To federal, state, local, tribal, territorial, foreign, or international agencies, if DHS determines (1) the information is relevant and necessary to the agency's decision concerning the hiring or retention of an individual, or the issuance of a security clearance, license, contract, grant, or other benefit, and (2) failure to disclose the information is

likely to create a risk to government facilities, equipment, or personnel; sensitive information; critical infrastructure; or the public safety.

BB. To federal, state, local, tribal, territorial, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest, for purposes related to administering or enforcing the law, national security, immigration, or intelligence, when consistent with a DHS mission-related function.

CC. To federal, state, local, tribal, territorial, or foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

DD. To foreign governments in order to notify them concerning an alien who is incapacitated, an unaccompanied minor, or deceased.

EE. To federal, state, local, tribal, and territorial courts or government agencies involved in criminal investigation or prosecution, pretrial services, sentencing, parole, probation, bail bonds, child welfare services, or any other aspect of the criminal justice process, and to counsel representing an individual in a criminal, civil, or child welfare proceeding, in order to ensure the integrity of the justice system by informing these recipients of the existence of an immigration detainer on that individual or that individual's status in removal proceedings, including removal, voluntary departure, or custodial status/location. Disclosure of that individual's Alien Registration Number (A-Number) and country of birth is also authorized to facilitate use of the ICE Online

Detainee Locator System by the aforementioned individuals and agencies. This routine use does not authorize disclosure to bail bond companies or agents.

FF. To appropriate federal, state, local, tribal, foreign or international criminal justice agencies, or other authorized users of NCIC, to respond to inquiries regarding a person who is or may be the subject of an ICE-generated NCIC criminal arrest warrant or immigration lookout record.

GG. 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 behind locked doors. Electronic records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by personal, biographic, or biometric identifiers such as

name, date of birth, place of birth, address, A-Number(s), FBI criminal history number(s), Social Security Number, Fingerprint Identification Number, and passport number.

**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 systems containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

ICE is seeking approval for a records retention schedule for the records described in this system of records. ICE proposes to maintain the IAQ and IAR records pertaining to criminal biometric and biographic immigration status checks and pertaining to National Sex Offender Registrants for seventy-five (75) years. The IAQ and IAR records pertaining to non-criminal biometric and biographic immigration queries will be kept for thirty (30) years. Records pertaining to Brady Act, special security event, and OPM checks will be kept for five (5) years from the date an immigration status determination is made and an IAR returned, after which the records will be deleted from the ACRIME system. ICE proposes to maintain NCIC Module records (containing the underlying basis for the ICE-generated NCIC record) for 75 years from the date the record is removed from NCIC. ICE also proposes to maintain Communication Center Module records containing NCIC Hit Confirmation calls for 75 years and follow-up calls to IARs for the

time period consistent with the type of query conducted. Additionally, ICE proposes to maintain tips and suspicious activity reporting in the Communications Center Module for ten (10) years from the date of the tip.

**System Manager and address:**

Unit Chief, Law Enforcement Support Center, U.S. Immigration and Customs Enforcement, 188 Harvest Lane, Williston, VT 05495.

**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 ICE'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 and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528-0655.

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 C.F.R. 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 Chief Privacy Officer and Chief Freedom of Information Act Officer, <http://www.dhs.gov> or 1-866-431-0486. In addition you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records.

If your request 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 the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

**Record access procedures:**

See “Notification procedure” above.

**Contesting record procedures:**

See “Notification procedure” above.

**Record source categories:**

Records are obtained from ICE and other federal, state, local, tribal, foreign, and international criminal justice agencies (e.g., law enforcement agencies, investigators,

prosecutors, correctional institutions, police departments, and parole boards).

**Exemptions claimed for the system:**

Pursuant to 5 U.S.C. § 552a(j)(2) of the Privacy Act, portions of this system are exempt from subsections (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) of the Privacy Act. In addition, the system has been exempted from subsections (c)(3), (d), and (e)(1), (4)(G), (4)(H), and (f) pursuant to 5 U.S.C. § 552a(k)(2). Rules have been promulgated in accordance with the requirements of 5 U.S.C. § 553(b), (c), and (e) and have been published in the Federal Register as additions to Title 28, Code of Federal Regulations (28 C.F.R. § 16.99). 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: January 24, 2013.

Jonathan R. Cantor,

Acting Chief Privacy Officer,

Department of Homeland Security.

**[FR Doc. 2013-03377 Filed 02/13/2013 at 8:45 am; Publication Date: 02/14/2013]**