



**Privacy Impact Assessment Update  
for the**

# **Alien Criminal Response Information Management System (ACRIME)**

**DHS/ICE/PIA-020(c)**

**September 28, 2018**

**Contact Point**

**Nathalie Asher**

**Executive Associate Director (A)**

**Enforcement and Removal Operations (ERO)**

**U.S. Immigration and Customs Enforcement**

**202-732-3300**

**Reviewing Official**

**Philip S. Kaplan**

**Chief Privacy Officer**

**Department of Homeland Security**

**202-343-1717**



## Abstract

The Alien Criminal Response Information Management System (ACRIME) is an information system used by U.S. Immigration and Customs Enforcement (ICE) headquarters and field personnel to receive and respond to immigration status inquiries made by other agencies about individuals arrested, subject to background checks, or otherwise encountered by those agencies. The original ACRIME Privacy Impact Assessment (PIA) was published on April 22, 2010, and has since been updated on September 29, 2010 and January 24, 2013.<sup>1</sup> ICE is updating this PIA again for the following reasons:

- To document that the ACRIME Field Module (“ACRIME Field” or “Field”) is being deployed to Enforcement and Removal Operations (ERO) Field Offices across the country;
- To indicate that the module formerly referred to as the National Crime Information Center (NCIC) Section Module is now called the Wants and Warrants Module;
- To describe the technical services that ACRIME uses to query other government databases for relevant information; and
- To explain that ICE is now using ACRIME to respond to inquiries submitted by the U.S. Department of Health and Human Services (HHS) regarding the immigration status of potential sponsors of unaccompanied alien children (UAC).

## Overview

The original ACRIME PIA published in 2010 describes the procedures followed by ICE personnel at the Law Enforcement Support Center (LESC) to process Immigration Alien Queries (IAQ) submitted by outside law enforcement agencies (LEA). LEAs submit IAQs to ICE when they want to confirm the immigration status of an investigation subject. After the LESL processed an IAQ, it could forward a copy of the Immigration Alien Response (IAR) back to the submitting LEA and, when appropriate, forward a copy to an ICE field office for follow-up action. The LESL processes IAQs within the ACRIME Modernization Module (“ACRIME Mod”). ACRIME Mod is referred to in the original ACRIME PIA as the ACRIME Operations Module. ACRIME Mod supports traditional law enforcement checks, Brady Act checks, special security event checks, and U.S. Office of Personnel Management (OPM) checks.

---

<sup>1</sup> See DHS/ICE/PIA-020 Alien Criminal Response Information Management System (ACRIME) and subsequent updates, available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).



### *ACRIME Field*

In fiscal year 2018, ICE deployed ACRIME Field to ERO offices across the country.<sup>2</sup> With ACRIME Field, ERO field office personnel now have a common, standardized application to receive, manage, and process<sup>3</sup> all IARs distributed to their offices. The LESC uses ACRIME Mod to perform database searches and route the results to ERO field offices. ACRIME Field users at the ERO field offices use LESC's search results when responding to the IAQ. When the LESC transmits IARs to ERO field offices, Field users can view, sort, filter, and search IARs in their location-specific queue (*i.e.*, ACRIME Field users in Atlanta cannot see IARs sent to the San Diego field office).<sup>4</sup> Field users can see all queries and search results compiled by the LESC (preventing users from having to re-run these searches), update IARs based on new information, and determine whether enforcement action is appropriate.

ACRIME Field users review the IAR and then update certain fields based on the information in the IAR. First, Field users will update the case status, which indicates whether ICE lodged a detainer against the alien, referred the case to the ERO Criminal Alien Program (CAP), or referred the case to an ERO Fugitive Operations team because the alien is currently at-large.<sup>5</sup> Second, Field users will update the disposition of the case (*e.g.*, alien issued notice to appear, alien not amenable to removal, reinstatement of prior removal order). The information from these two fields provides guidance to downstream users on continuing the case to completion. Finally, ACRIME Field's connection with the Enforcement Integrated Database (EID) will enable a field

---

<sup>2</sup> The nationwide deployment of ACRIME Field includes the ICE Pacific Enforcement Response Center (PERC), ERO field offices, and ERO command centers.

<sup>3</sup> Processing an IAR consists of:

- Reviewing and verifying the summary data in the IAR;
- Conducting additional investigation/research that the officer deems necessary to obtain more information that can inform a decision on enforcement action;
- Determining whether to take enforcement action against an individual (*e.g.*, lodge detainer, refer to a Fugitive Operations Team, refer to the Criminal Alien Program);
- Inputting data into another ICE system, if appropriate (*e.g.*, EAGLE); and
- Informing the appropriate Field Office of the determination for further enforcement action.

<sup>4</sup> Once the appropriate field office has reviewed and processed the IAR, it goes to the "Completed Queue." Completed IARs can be searched and viewed by any field office.

<sup>5</sup> In ACRIME Field, the "Case Status" field has four possible options.

- **No Action:** The circumstances of the case do not warrant immigration enforcement action.
- **Criminal Alien Program (CAP) Referral:** The subject may warrant enforcement action, but he or she requires an interview by a field team. Or, the subject is currently in pending criminal proceedings, the outcome of which could warrant follow-up enforcement action.
- **At-Large Referral:** The subject warrants immigration enforcement action, but he/she has been determined to have been released from the custody of state/local law enforcement.
- **Detainer:** An ICE Form I-247A *Immigration Detainer* has been issued for the subject and is available for review in EAGLE.



user to start an encounter in the EID Arrest Graphical User Interface for Law Enforcement (EAGLE),<sup>6</sup> as explained below.

Prior to ACRIME Field, the LESC routed IARs to ERO field offices in one of three ways: (1) a dedicated, secure email account; (2) a custom SharePoint site; or (3) by using the same terminal that is used by the LESC to receive IAQs from state and local LEAs. Although ERO field offices would receive the IAR itself, they could not see the searches or queries that the LESC ran to generate the IAR.<sup>7</sup> This shortcoming required ERO field officers to re-run the same queries the LESC had already conducted. ACRIME Field significantly reduces this redundancy.

### ***ACRIME Field Integration with EID/EAGLE***

Before ACRIME Field deployed, ERO field officers or authorized support staff received IARs from the LESC, and then manually entered relevant information into EAGLE.<sup>8</sup> Information in EAGLE is automatically saved and stored in EID.<sup>9</sup> ACRIME Field allows for greater integration with EID. When the LESC returns the IAR and all search results to the ERO field office, Field users can click a button in ACRIME Field to create a new entry in EID. Because information stored in EID can be retrieved using EAGLE, certain IAR data points are automatically transmitted to EAGLE. Therefore, when ERO officers use EAGLE to create a detainer on an investigation subject, the ICE Form I-274A detainer form will auto-populate with most of the required information, eliminating the need for manual entry.

ACRIME Field includes functionality to update an existing record or create a new record in EID/EAGLE. When an ACRIME Field user processes an IAR on an alien who ICE has previously encountered, the user will have the option of updating a narrative field in the alien's case file in EAGLE to describe the latest encounter, how the alien came to ICE's attention, and the alien's criminal and immigration status. ACRIME Field will transfer approximately 30 data points common to both ACRIME and EID (*e.g.*, name, Alien Registration Number, date of birth) from the IAR and search results to EID/EAGLE as a means of starting an immigration case. The transfer of information from ACRIME to EID does not create new EID data fields, but instead adds to existing EID data fields. ACRIME Field users can also create a new encounter and subject record for any aliens who ICE has not previously encountered. In addition, if the disposition of an IAR

---

<sup>6</sup> See DHS/ICE/PIA-015(e) EAGLE, available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>7</sup> The IAR provides only basic, summary information about the immigration and criminal history of the individual being queried. It does not provide a sufficient level of detail and scope on that individual for an ERO officer to determine whether to take enforcement action (*e.g.*, lodge a detainer, refer to an ERO Criminal Alien Program team, refer to an ERO Fugitive Operations team).

<sup>8</sup> EAGLE, a subsystem of the Enforcement Integrated Database (EID), is a booking application used by ICE law enforcement officers to process the biometric and biographic information of individuals arrested by ICE. The EAGLE PIA is available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>9</sup> See DHS/ICE/PIA-015 Enforcement Integrated Database (EID), available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).



results in an encounter (such as lodging a detainer), this will also be reflected in EID. This function will increase efficiency and enhance data quality for ERO.

### *Access and User Roles*

ACRIME Field uses Single Sign-On (SSO) to validate ICE users with Personal Identity Verification (PIV)-card authentication. SSO is a method of access control that enables a user to log in at a single point and gain access to the resources of multiple software systems by using credentials stored on shared, centralized authentication servers. PIV-card authentication provides an extra layer of security by storing a user's SSO credential on a physical card that must be present at login. This reduces the risk of unauthorized access, and therefore, unauthorized sharing, and also enables tracking and auditing of user activity.

Depending on whether the ACRIME Field user is an ERO officer, or ERO supervisor, or a contractor supporting ERO, different permissions and restrictions apply. For example, ERO officers are permitted to view active IARs in their Area of Responsibility (AOR), search completed IARs from any field office, amend a previously completed IAR, and conduct a data quality check. Supervisors have all the permissions of ERO officers, plus the ability to view the Supervisor Dashboard, to see IAR statistics, and to assign IARs to specific users. Finally, contractors have limited access to ACRIME Field. Contractors triage incoming cases so that all IARs are reviewed and routed timely to officers. Contractors cannot amend IARs, conduct data quality checks, or mark an IAR as "complete."

### *ACRIME Field Interface*

When ACRIME Field users log in, they see a screen titled "Active Queue." The Active Queue is used to receive and process recently received IARs. IARs automatically appear in reverse chronological order by 'Received Time,' meaning the most recent IAR will be on top. The Active Queue displays the following information related to the IAR:

- Name;
- Alien Registration Number ("A-Number");
- Federal Bureau of Investigation (FBI) Number;
- Date of birth;
- Criminal Offense Level (1-3);<sup>10</sup>

---

<sup>10</sup> ICE uses criminal history information to classify aliens charged with or convicted of a criminal offense into one of three ICE levels. For a full discussion of Criminal Offense Levels, see DHS/ICE/PIA-020(a) Alien Criminal



- Query ID number (unique ACRIME identifier);
- Name of ERO officer and/or contractor assigned to the IAR;
- Area of Responsibility (AOR) and Docket Control Office (DCO) of the IAR;
- IAR status (pending, pending completion, completed, or amended);
- Custody status (whether the alien was noted as being in the custody of local law enforcement at the time of the IAQ submission);
- Case status; and
- Subject's immigration status (*e.g.*, lawful permanent resident, non-immigrant).

The information in this queue comes from data in the IAQ, the response from the LESC, and activity from the ACRIME Field user. Further, the Active Queue does not give ACRIME Field users, either ERO or contractors, access to any data elements that they cannot already view in other systems, such as EAGLE or other civil and criminal information databases.

ACRIME Field users can also search for an IAR by filling out any or all of the following fields: name, date of birth, Social Security number, FBI Number, A-Number, or Query ID number. As a default setting, the Active Queue will only show IARs for the ACRIME Field user's AOR. After searching, ACRIME Field users can "check out" an IAR to make appropriate edits and complete IAR processing. ERO officers and supervisors then click a button in ACRIME Field marked "DQI" (short for Data Quality and Integrity), indicating that they have reviewed the case for accuracy. If the officer or supervisor makes changes during the data quality check, the IAR will be marked "amended." Once an IAR has been processed, it then moves to the "Completed Queue." Field users can search the Completed Queue to view any IAR, regardless of which field office to which it was originally assigned.<sup>11</sup> Finally, ACRIME Field users can create a PDF of the completed IAR to print or review offline.

### ***Wants and Warrants Module***

The original ACRIME PIA discussed the National Crime Information Center (NCIC) Section Module, which is used to create, update, and clear<sup>12</sup> records in the FBI's NCIC system.

---

Response Information Management System (ACRIME) and subsequent updates, *available at* [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>11</sup> This might be necessary when field users in other AORs or Headquarters need to conduct a historical search on a subject.

<sup>12</sup> A record is "cleared" when it is no longer accurate or no longer needed in the FBI's NCIC system. If this is the case, the record will be removed from NCIC files either because the individual was apprehended or because the information in the record is no longer current.





Since the publication of the original ACRIME PIA, the NCIC Section Module has been renamed the “Wants and Warrants Module.” Within ICE, only the LESC uses this module of NCIC.

The Wants and Warrants Module provides authorized ACRIME users with an automated method to manage ICE data exchange with the NCIC Warrants Service. ICE uses this module to manage records of aliens for whom there is an outstanding criminal or administrative warrant or for whom ICE has placed a “lookout.”<sup>13</sup> NCIC maintains lookout records for individuals with a criminal warrant, those who may try to re-enter the United States after being removed, and for aliens who fail to appear for removal proceedings. If ICE seeks an investigation subject who has no record in NCIC, then ACRIME users at the LESC can request to enter information in NCIC about that individual.

### *ACRIME Technical Services*

The original ACRIME PIA discussed how ACRIME users could query federal law enforcement agency databases for information about the alien’s immigration status and criminal history. ACRIME uses three federal agency web services to query and retrieve relevant data from federal law enforcement agency information systems. The federal agency web services are:

- The NCIC-National Law Enforcement Telecommunications System (NLETS) Web Service (NNWS);
- the External Search Service (ESS); and
- the Person Centric Query Service (PCQS).<sup>14</sup>

These web service search options have been used since ACRIME was first developed but were not described in previous versions of the ACRIME PIA. With this update, ICE is identifying the specific databases that ERO queries.

NNWS uses a connection between the NLETS and the FBI’s NCIC. ICE uses NNWS to update a subject’s criminal record in FBI’s NCIC system, to connect to the Wants and Warrants Module, and for data exchange. Specifically, NNWS is used to query FBI’s NCIC system to receive criminal history information for the requested subject. NNWS is also used to distribute IARs back to the requesting agency and to submit updates to FBI lookout files.

ESS provides data retrieval services to ACRIME users. It allows them to connect to multiple law enforcement and immigration systems to provide comprehensive immigration

---

<sup>13</sup> ICE can place a “lookout” either for an individual or for an article. For example, ICE may place a lookout for an individual being sought for removal or for a missing, lost, or stolen item (e.g., firearm, badge, radio).

<sup>14</sup> ICE owns both NNWS and ESS. United States Citizenship and Immigration Services (USCIS) owns PCQS. See DHS/USCIS/PIA-010 Person Centric Query Service (PCQS) and subsequent updates, *available at* [www.dhs.gov/privacy](http://www.dhs.gov/privacy).



information. ACRIME users use ESS and PCQS to query the following federal information systems to respond to IAQs:

- Central Index System (CIS) – owned by United States Citizenship and Immigration Services (USCIS);<sup>15</sup>
- Computer Linked Application Information Management System (CLAIMS 3 and 4) – owned by USCIS;<sup>16</sup>
- Enforcement Integrated Database (EID) – owned by ICE;<sup>17</sup>
- Automated Biometric Identification System (IDENT) – owned by the National Protection and Programs Directorate (NPPD);<sup>18</sup>
- Arrival and Departure Information System (ADIS) – owned by U.S. Customs and Border Protection (CBP);<sup>19</sup>
- Student Exchange Visitor Information System (SEVIS) – owned by ICE;<sup>20</sup> and
- Executive Office for Immigration Review (EOIR) database – owned by the Department of Justice (DOJ).<sup>21</sup>

### *IAQs of Potential UAC Sponsors*

In 2018, ICE ERO entered into a Memorandum of Agreement (MOA) with the U.S. Department of Health and Human Services (HHS) Office of Refugee Resettlement (ORR). Under the MOA, ICE has agreed to verify the immigration status and provide limited criminal history information of potential sponsors of UACs who are currently in HHS custody and other adult members of the potential sponsors' households. ERO will use ACRIME to query appropriate government databases to provide HHS with the pertinent immigration status and criminal history information. ICE will only share criminal history information with HHS when there is criminal history associated with the individual. The criminal history information that ICE shares is limited

---

<sup>15</sup> See DHS/USCIS/PIA-009 Central Index System (CIS) and subsequent updates, available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>16</sup> See DHS/USCIS/PIA-015 Computer Linked Application Information Management System (CLAIMS 4) and subsequent updates and DHS/USCIS/PIA-016 Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems, available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>17</sup> See DHS/ICE/PIA-015 Enforcement Integrated Database (EID), available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>18</sup> See DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) and Appendices, available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>19</sup> See DHS/CBP/PIA-024 Arrival and Departure Information System, available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>20</sup> See DHS/ICE/PIA-001 Student and Exchange Visitor Information System (SEVIS) and subsequent updates, available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>21</sup> See Case Access System for EOIR, available at <https://www.justice.gov/opcl/doj-privacy-impact-assessments>.





to the individual's FBI number, State ID number, the NCIC number associated with a lookout in FBI's NCIC system, and the Criminal Offense Level. This information may be used to inform an HHS determination whether to grant or deny a sponsorship application.

## Reason for the PIA Update

The PIA for ACRIME was last updated on January 24, 2013. ICE has since modernized ACRIME to be used by ERO field offices, to track outstanding warrants and lookouts, and to employ web services that help ACRIME users respond to IAQs.

## Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

### Authorities and Other Requirements

Authority for maintenance of the system is provided in 8 U.S.C. §§ 1103, 1226, 1227, 1228, 1231, 1232, 1357 and 1360; the Brady Handgun Violence Protection Act of 1993 (Pub. L. No. 103-159); and DHS Delegation Number 7030.2, Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003).

The DHS/ICE-007 Criminal History and Immigration Verification (CHIVe) System of Records Notice (SORN) applies to the information contained in the ACRIME system.<sup>22</sup>

A system security plan has been completed for ACRIME. This was last updated on March 14, 2017.

Records in ACRIME are covered by Records Schedule DAA-0567-2017-0002, which has been approved by the National Archives and Records Administration (NARA).<sup>23</sup> The specific retention periods for ACRIME records are discussed below.

---

<sup>22</sup> See DHS/ICE-007 Criminal History and Immigration Verification (CHIVe) System of Records, 83 FR 20844 (May 8, 2018), available at <https://www.federalregister.gov/documents/2018/05/08/2018-09902/privacy-act-of-1974-system-of-records>.

<sup>23</sup> See [https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2017-0002\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2017-0002_sf115.pdf).



### **Characterization of the Information**

ACRIME ingests information from the federal information systems identified in the “ACRIME Technical Services” section of this PIA update. When law enforcement agencies submit IAQs to ICE via NLETS, an LESC ACRIME Mod user uses the web services identified above to query the appropriate federal information systems for relevant information about the individual. ICE returns the information to the requesting LEA via NLETS in the form of an IAR. The LEAs submitting IAQs to ICE generally collect information directly from the individual. An ACRIME Field user can then access the search results in ACRIME Field and make an appropriate enforcement determination.

As indicated in the original ACRIME PIA, the system also collects information in the ACRIME Communications Center Module regarding phone calls received by the LESC. This module collects PII about both the subject of the call (i.e., the alien about whom the requestor wants information) and about the caller him/herself. ACRIME does not use information from commercial sources or publicly available data.

**Privacy Risk:** There is a risk that ICE collects more information than is necessary for the purpose of screening potential UAC sponsors and other adult members of those sponsors’ households.

**Mitigation:** This risk is mitigated. ICE cannot process IAQs pertaining to potential UAC sponsors (and other adult members of those sponsors’ households) without receiving relevant biographic and biometric information. In order to properly inform HHS of the sponsor’s immigration history and limited criminal history, ICE needs to collect PII to query other government databases. All PII collected is necessary to fulfill the purposes of the MOA with HHS and is narrowly tailored to effectively convey information.

### **Uses of the Information**

With this update, ICE has expanded the users of ACRIME beyond the LESC to include ERO officers located at the Pacific Enforcement Response Center (PERC) as well as in ERO field offices and command centers across the country. By implementing ACRIME Field, ERO now has additional information to aid in its determination of the course of immigration enforcement actions. For example, a state or local LEA may send an IAQ to the LESC via NLETS, asking about the immigration status of a particular subject. The LESC then queries the appropriate federal information systems to generate the IAR and then responds to the LEA that the subject in question may be in the country illegally. The LESC then uses ACRIME Field to send the IAR (including the queries run to generate the IAR) to the appropriate ERO field office. ERO officers in the field will receive the information via ACRIME Field and determine whether ICE needs to detain the subject, dispatch a fugitive operations team, or take other enforcement action.



ICE also uses ACRIME to respond to IAQs regarding potential UAC sponsors and other adult members of the sponsors' households. While the process of creating an IAR and sending the response back to the originating agency remains the same, it is important to identify this new class of individuals whose information will be maintained in ACRIME.

**Privacy Risk:** There is a risk that the system does not protect against unauthorized use.

**Mitigation:** Only authorized ICE users with a need to know have access to ACRIME and the PII contained within the system. User access roles are determined by the employee's or contractor's position, which ensures that users are granted only as much access as is necessary to perform their official duties. Additionally, user access is granted only through an ACRIME system administrator. Only authorized ICE employees and contractors can access ACRIME and the data maintained within the system.

In this case, ERO officers located at either the PERC or field offices or command centers across the United States require ACRIME access to perform their official duties. Access to ACRIME Field allows ERO officers to determine the immigration status of investigation subjects encountered by state or local LEAs and determine whether any further action is required by ICE.

### **Notice**

The publication of this PIA update and the CHIVE SORN give notice to members of the public that their information may be stored in ACRIME. Due to the law enforcement and immigration purposes for which the information is collected, opportunities for individuals to be notified prior to the collection of information may be limited or nonexistent. Individuals may be notified that their information may be shared for law enforcement purposes by other LEAs at the time their data is collected. Additionally, ACRIME users do not collect information directly from the subject under investigation; the information is either provided by another LEA or retrieved from the federal information systems listed above. Those government systems are responsible for providing notice (as appropriate) to individuals whose information may be collected. Therefore, as it pertains to ACRIME, ICE is not in the best position to provide notice to individuals about the collection of their information.

**Privacy Risk:** There is a risk that potential UAC sponsors and other adult members of their households are not aware that ICE is providing their immigration status and criminal history to HHS for screening purposes.

**Mitigation:** This risk is partially mitigated. When individuals apply to sponsor a UAC, they must provide information to HHS by completing various forms. These forms notify potential sponsors that their information may be shared with other federal agencies, which includes ICE. However, other adult members of the sponsors' households are not required to personally complete the forms, and therefore may not receive appropriate notice. In some cases, the potential sponsors may provide information about other adult members of their households. The publication of this



PIA update and the CHIVE SORN provide notice to UAC sponsors and other adult members of the sponsors' households that ICE will provide immigration status and criminal history information to HHS, and that HHS may use that information in deciding whether to grant or deny a sponsorship application.

### **Data Retention by the project**

ICE maintains records in ACRIME for either 5 years or 75 years depending on the type of information contained in the record. The following retention periods apply to records covered in ACRIME:

#### *Records maintained for 75 years (and then destroyed)*

- IAQ and IAR records for traditional law enforcement checks;
- IAQs and IARs pertaining to non-criminal biographical and biometric investigations; and
- ICE-generated FBI NCIC records.

#### *Records maintained for 5 years (and then destroyed)*

- IAQ and IAR records pertaining to Brady Act checks;
- IAQ and IAR records pertaining to special security event checks; and
- IAQ and IAR records pertaining to OPM checks.

Finally, ICE proposes to maintain IAQ and IAR records pertaining to potential UAC sponsors (and other adult members of the potential sponsors' households) for 5 years. Until NARA approves a records schedule for that group of records, they will be treated as permanent and cannot be deleted.

ICE has not identified any new risks related to data retention.

### **Information Sharing**

With this update, ICE will now share immigration status and limited criminal history information with HHS as it pertains to potential sponsors of UACs and other members of the adult sponsors' households. If a potential sponsor (or other adult member of the sponsor's household) has no associated criminal history, then ICE will only provide the immigration status of that individual. If there is criminal history associated with the individual, then ICE shares the following information with HHS:



- FBI Number;
- State ID Number;
- the NCIC number associated with a lookout in FBI's NCIC system; and
- Criminal Offense Level.

HHS must then use the identifying numbers provided by ICE to query other databases and obtain the individual's complete criminal history. HHS may use this information in deciding whether to grant or deny a sponsorship application. This information sharing is consistent with Routine Use HH of the CHIVe SORN.<sup>24</sup>

**Privacy Risk:** There is a risk that HHS will use ICE information beyond the purposes outlined in the MOA and described in this PIA.

**Mitigation:** This risk is partially mitigated. First, ICE only shares immigration status and, in some cases, very limited criminal history information regarding potential UAC sponsors and other adult members of the sponsors' households. The information provided by ICE is the minimum amount necessary to inform an HHS determination whether to grant or deny a sponsorship application. Second, the MOA between ICE and HHS is clear regarding its scope and purpose, which indicates how HHS will use the information provided by ICE. If ICE learns that HHS is using this information beyond the purposes outlined in the MOA, it can terminate the agreement. However, after ICE transmits the relevant information to HHS, ICE is not able to control how HHS uses that information.

**Privacy Risk:** There is a risk that ICE may share information from ACRIME that is protected from disclosure by statute (e.g., information protected under 8 U.S.C. § 1367).

**Mitigation:** The ACRIME system itself does not have a means to screen individuals for protection under 8 U.S.C. § 1367 (i.e., applicants or beneficiaries under the Violence Against Women Act, or applicants or beneficiaries of a T or U visa). However, ACRIME personnel are trained in following appropriate protocols regarding this information to ensure that ICE is not disclosing any information in violation of law, regulation, or policy. When ACRIME users query the government systems listed above (e.g., CLAIMS, CIS), those systems will indicate whether the subject of an IAQ is protected by this statute. ACRIME personnel only disclose information in accordance with law, policy, and regulation, including DHS Instruction 002-02-001 "Implementation of Section 1367 Information Provisions" (Nov. 7, 2013).

---

<sup>24</sup> (HH) To HHS, the citizenship or immigration status, immigration history, criminal history information, and other biographic information of potential sponsors for unaccompanied alien children and other adult members of the potential sponsors' households to inform an HHS determination regarding the sponsorship of an unaccompanied alien child.



### Redress

The right to request access to and amendment of records under the Privacy Act of 1974 (5 U.S.C. §552a) is limited to United States citizens and lawful permanent residents. Executive Order 13768 *Enhancing Public Safety in the Interior of the United States* (January 25, 2017) states: “Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.”<sup>25</sup> This Executive Order precludes DHS from extending such rights by policy. The Judicial Redress Act of 2015 (5 U.S.C. §552a note), which amended the Privacy Act, provides citizens of certain countries with access, amendment, and other redress rights under the Privacy Act in certain limited situations.<sup>26</sup>

As a result of Executive Order 13768, DHS’s “Mixed Systems Policy”<sup>27</sup> was rescinded by the DHS Privacy Office in its Privacy Policy Guidance Memorandum (April 25, 2017).<sup>28</sup> However, DHS will consider individual requests to determine whether or not an individual may access or amend records contained in this system. Individuals seeking access to and notification of any records contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE Freedom of Information Act (FOIA) Officer. Individuals who wish to contest the accuracy of records in the system may submit these requests to the ICE Privacy Division.

In addition, the DHS Privacy Policy Guidance Memorandum makes clear that DHS has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes. Failure to maintain accurate records serves to undermine efficient decision making by

---

<sup>25</sup> The full text of Executive Order 13768 can be found here: <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>.

<sup>26</sup> The foreign countries and regional organizations covered by the Judicial Redress Act include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the U.S. Department of Justice website <https://www.justice.gov/opcl/judicial-redress-act-2015>.

<sup>27</sup> The DHS’ “Mixed Systems Policy” extended most Privacy Act protections to visitors and aliens whose information was collected, used, maintained, or disseminated in connection with a mixed system of records (i.e., contains PII on both U.S. citizens and lawful permanent residents, as well as non-U.S. citizens and non-lawful permanent residents).

<sup>28</sup> DHS Memorandum 2017-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 25, 2017) (DHS Privacy Policy), available at <https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01>. As the DHS Privacy Policy notes, Executive Order 13768, does not affect statutory or regulatory privacy protections that may be afforded to aliens, such as confidentiality rights for asylees and refugees, and individuals protected under 8 U.S.C. §1367. These laws operate independently of the Privacy Act to restrict federal agencies’ ability to share certain information about visitors and aliens, regardless of a person’s immigration status.





DHS personnel, and can create the risk of errors made by DHS and its personnel. Also, PIAs are published, in part, to ensure that projects, programs, and systems maintain accurate data.

**Privacy Risk:** There is a risk that individuals (including UAC sponsors and other adult members of the sponsors' households) will be unable to participate meaningfully in the use of their data as maintained in this system, or determine whether the system maintains records about them.

**Mitigation:** This cannot be fully mitigated. Because data stored in ACRIME is maintained for a law enforcement purpose, individuals' rights to be notified of the existence or non-existence of data about them, and to direct how that data may be used by ICE, are limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools, such as wiretaps or surveillance, will no longer be useful. Permitting individuals to direct the agency's use of their information will similarly interfere with the intended law enforcement use of the system. Nevertheless, the publication of this PIA update and associated SORN provides general notice about ICE's collection of information, and how that information is used. In addition, in exempting its investigative systems from access and amendment under the Privacy Act, ICE has indicated that the exemptions will be applied on a case-by-case basis at the time of the access or amendment request. In appropriate circumstances, therefore, individuals may have an opportunity to access or correct their records, consistent with law enforcement necessity.

### **Auditing and Accountability**

This PIA update does not change the auditing process for use of the ACRIME system. Because ICE processes IAQs pertaining to UAC sponsors (and other adult members of their households) in the same manner as traditional law enforcement IAQs, the auditing controls remain the same. System administrators continue to monitor user account access by ensuring that only those with a need to know are granted access to the system. System users are validated using single sign-on (SSO) with PIV-card authentication after an administrator has granted appropriate access. System administrators will remove the credentials for individuals who no longer require access or no longer have a need to know the information in the system.

To ensure data quality and integrity, ERO supervisors review information entered in ACRIME Field, and can click a box labeled "DQ" when the data quality check is complete. Further, downstream users of the information can also amend data fields if new information becomes available.

Finally, all ACRIME users (both federal employees and contractors) continue to take mandatory training, including privacy and security training. This helps to ensure that all system users handle PII appropriately and that they understand how to safeguard the information contained



within the system. Users must also take application specific (Mod, Field, Wants and Warrants, etc.) training prior to being granted access.

## **Responsible Official**

Lauren Berkebile  
Acting Privacy Officer  
U.S. Immigration and Customs Enforcement  
Department of Homeland Security

## **Approval Signature**

[Original signed copy complete and on file with DHS Privacy Office]

---

Philip S. Kaplan  
Chief Privacy Officer  
Department of Homeland Security