Privacy Impact Assessment Update
for the

Alien Criminal Response Information Management System (ACRIMe) & Enforcement Integrated Database (EID)

September 29, 2010

Contact Point
James A. Dinkins, Executive Associate Director
Office of Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Alien Criminal Response Information Management System (ACRIMe) is an information system used by U.S. Immigration and Customs Enforcement (ICE) 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 Enforcement Integrated Database (EID) is an ICE case management system that captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and U.S. Customs and Border Protection. ICE is combining ACRIMe and EID data via the ICE Integrated Decision Support (IIDS) System, a reporting sub system of EID, to enable and enhance comprehensive reporting about criminal aliens throughout the alien identification, apprehension, and removal process. To effectuate this reporting, ICE is modifying ACRIMe to expand its user base within the agency, implementing new user functionality in ACRIMe and EID, and updating IIDS to support enhanced reporting of ACRIMe and EID data. ICE is further expanding ACRIMe support for the Secure Communities initiative. ICE is conducting this PIA update to address these modifications and enhancements.

Introduction

With the publication of this PIA update, ICE is modifying two of its information technology (IT) systems–ACRIMe and EID (including IIDS, an EID reporting sub system)–to support enhanced, comprehensive reporting of the criminal alien identification, apprehension, and removal process. For consistent reporting across both systems and prioritization purposes throughout the process, ICE has implemented a risk-based approach to immigration enforcement that seeks to identify aliens charged with or convicted of a criminal offense and remove them from the United States when possible. To implement this approach, ICE uses criminal history information to classify aliens charged with or convicted of a criminal offense into the following three ICE Levels:[1]

- Level 1–Aliens convicted of "aggravated felonies," as defined in § 101(a)(43) of the Immigration and Nationality Act, or two or more crimes each punishable by more than one year, commonly referred to as "felonies". Examples include major drug offenses, national security crimes, and violent crimes such as murder, manslaughter, rape, robbery and kidnapping.

- Level 2–Aliens convicted of any felony or three or more crimes each punishable by less than one year, commonly referred to as "misdemeanors." Examples include minor drug and property offenses such as burglary, larceny, fraud, and money laundering.

- Level 3–Aliens convicted of crimes punishable by less than one year.

The ICE Levels are only used for prioritization purposes and do not determine an individual's eligibility for removal. Aliens charged with or convicted of multiple criminal offenses may be "promoted" to a higher level for purposes of prioritization. For instance, an individual convicted of two ICE Level 2

---

[1] ICE Policy Number 10072.1, *Civil Immigration Enforcement: Priorities for the Apprehension, Detention, and Removal of Aliens*, June 30, 2010. http://www.ice.gov/doclib/civil_enforcement_priorities.pdf

offenses becomes an ICE Level 1. Although ICE Levels are based on convictions, ICE also applies ICE Levels to aliens charged with a criminal offense in order to manage ICE's workload, resources and enforcement activities.

The modifications to both ACRIMe and EID (described below) support the assignment of ICE Levels to aliens charged with or convicted of criminal offenses and the associated reporting requirements. First, ICE is adding ACRIMe data to the existing IIDS system, which is used for statistical reporting of ICE immigration enforcement matters and previously only held data from EID.[2] By combining ACRIMe and EID data in IIDS, ICE enhances its ability to report on the identification, apprehension, detention, and removal of criminal aliens at various stages of the immigration enforcement process. These changes will help carry out ICE's enforcement priorities described above, help ensure that ICE resources are aligned with these priorities, and allow ICE to improve internal evaluations and public reporting on the performance of programs like the Law Enforcement Support Center (LESC) and Secure Communities.

This PIA update also describes other enhancements to ACRIMe and EID. ICE is modifying ACRIMe to expand its user base to ICE field offices throughout the United States and implement new functionality that allows users to "refresh" a previously processed Immigration Alien Query (IAQ) and Immigration Alien Response (IAR) to update information about the subject. ICE is also updating EID's ENFORCE Apprehension Booking Module (EABM) to allow users to manually enter criminal history information about a person arrested by ICE, which will be used to calculate the appropriate ICE Level.

These enhancements and modifications are described below in more detail.

Reporting via the ICE Integrated Decision Support (IIDS) System

IIDS is a sub system of EID that functions as a data repository and contains a subset of data from the EID database. ICE uses IIDS for generating standard operational and executive level reporting (e.g., performance management and statistics) and *ad hoc* reports as necessary. On a daily basis, data is extracted from EID and uploaded into IIDS using an extraction, transformation and loading (ETL) process, which removes duplicative records about the same individual and reduces the information to only those data fields necessary for reporting purposes. With the publication of this update, ICE is changing the data fields that are sent to IIDS from EID records to include the ICE Level and criminal history information (e.g., National Crime Information Center [NCIC] codes, prior arrests and convictions, charge information, etc.) that will now be captured in EID (as described below).

IIDS receives certain data elements from ACRIMe IAQ records, including PII such as name, date of birth, place of birth, criminal history information, and immigration status. With the publication of this PIA update, IIDS will also receive ICE Levels assigned by ICE personnel when processing an IAQ in ACRIMe (described below). ACRIMe data will be extracted and uploaded into IIDS on a monthly basis with near-real time updates available as necessary for *ad hoc* reporting purposes, such as Secure Communities statistics for Congressional quarterly reports.

ICE uses IIDS to automatically match the ACRIMe data with the EID data. During the ETL process, the ACRIMe and EID data are matched using a combination of personal identifiers and other data fields such as name, date of birth, gender, alien registration number (A-number), FBI number, and

---

[2] For a description of IIDS, see the DHS PIA *Enforcement Integrated Database* (Jan. 14, 2010). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf.

fingerprint identification number (FIN). Once the matching is complete, the information is uploaded and available in IIDS for generating reports. This matching enables ICE to track the ICE Levels for aliens at different stages in the immigration enforcement process, such as when they are first identified (i.e., via an IAQ processed by ACRIMe), when ICE arrests them (i.e., an arrest record entered into EID via EABM), and when ICE removes them from the United States (i.e., a removal record entered into EID via the ENFORCE Alien Removal Module). Generally, the ICE Levels assigned to IAQs in ACRIMe match the ICE Levels generated in EID because the criminal history information used to determine the ICE Level is the same. It is possible the criminal history information could change between the time ICE processes an IAQ and when it apprehends and/or processes the same individual for removal from the United States. In this event, the ETL process reconciles the disparate ICE Levels defaulting to the ICE Level generated or assigned based on the most current and updated criminal history information.

With the addition of the data described above, IIDS will be able to generate statistical reports that support a comprehensive, end-to-end reporting of the criminal alien identification, apprehension, and removal process. ICE will use this reporting capability internally to ensure its resources are allocated appropriately and that ICE enforcement activities are aligned with ICE priorities, and externally to provide more comprehensive data to Congress and the public.

ACRIMe Enhancements

With this update, ICE will deploy ACRIMe to ICE field offices to support the increased volume of IAQs ICE receives due to the continued deployment of Interoperability[3] to state and local law enforcement communities via the Secure Communities initiative. ACRIMe will automatically distribute IAQs to the appropriate ICE field office by geographic area based on the originating agency identifier (ORI) number provided by the requesting criminal justice agency in the IAQ. ACRIMe users will primarily process IAQs pertaining to their geographic area, however, for back-up support and business continuity purposes ACRIMe users will be able to assist in processing workloads assigned to other geographical areas as necessary. Field office ACRIMe users will be able to process IAQs in the same manner the LESC does currently (described in the April 2010 ACRIMe PIA). Field users are also allowed to create new IAQs in the system as needed to run immigration checks on individuals they encounter.

ACRIMe will also allow users to reprocess or "refresh" previously reviewed IAQs/IARs using the automated searching capabilities of the ACRIMe Operations Module and information provided in the IAQ (e.g., name, alias, date of birth, etc.) as well as information previously gathered via ACRIMe. This re-vetting capability allows ICE personnel to check for updates in source systems, and to perform quality checks by verifying the accuracy of previously processed IARs.

Finally, ACRIMe will also allow users to assign ICE Levels to IAQs/IARs in the system. First, ACRIMe users will review the criminal history information gathered via ACRIMe's connection to NCIC. Based on the subject's criminal history and the current charge provided in the IAQ, users then determine the appropriate ICE Level using the ICE Level Mapping, which maps all NCIC criminal offense codes to

---

[3] A more detailed explanation of the IAFIS-IDENT interoperability process can be found in the DHS PIA *United States Visitor and Immigration Status Indicator Technology (US-VISIT) Program for the First Phase of the Initial Operating Capability of Interoperability between DHS and the U.S. Department of Justice* (Oct. 28, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_phase1ioc.pdf.

the appropriate ICE Level.[4]   As necessary, users will increase the ICE Level for multiple convictions consistent with ICE enforcement priorities. Then users will select the appropriate ICE Level from a drop-down menu in ACRIMe (i.e., Level 1, 2, 3 or Not Applicable).   Once the ACRIMe user finishes processing the IAQ, the ICE Level will be returned to the requestor as part of the IAR. Additionally, on a monthly basis, ACRIMe data will be extracted and loaded in IIDS for reporting purposes (as described above).

ENFORCE Apprehension Booking Module (EABM) Enhancement

ICE is updating EID's ENFORCE Apprehension Booking Module (EABM), which creates the booking record for persons arrested by ICE for violations of the Immigration and Nationality Act. This modification will allow EID users to manually enter criminal history information into the EABM booking record. Once entered, the system uses the criminal history information to automatically calculate the appropriate ICE Level based on the ICE Level Mapping coded into the system. The incorporation of the ICE Level information into booking records helps ICE law enforcement personnel in the field prioritize their enforcement activities on high-priority criminal aliens in line with ICE's enforcement policies.

At the time of arrest an ICE officer will logon to EABM and click the new "Crime Entry Screen," which will present a data entry screen where the officer can manually enter the alien's criminal history information (e.g., NCIC codes, crime description, current charge, prior arrests and/or convictions, disposition data, etc.). This information is typically gathered from NCIC and TECS. The system will automatically calculate an ICE Level (using the ICE Level Mapping described earlier) for each crime entered such as prior arrests, convictions and current charges. The ICE Level(s) will appear in EABM and the officer will use it to prioritize his enforcement activities in accordance with ICE policy. Additionally, on a daily basis, EID data including encounter records entered into EABM is extracted and loaded into IIDS for reporting purposes (described above).

Reason for the PIA Update

The original ACRIMe and EID PIAs were published on April 22, 2010 and January 14, 2010, respectively. Since then, user needs have changed and new reporting requirements have been established. ICE is implementing the enhancements and modifications described in this PIA update to address these needs. ICE is conducting this PIA update to address the expansion of ACRIMe's user base within the agency, implementing new user functionality in ACRIMe and EID, and updating IIDS to support enhanced reporting of ACRIMe and EID data. ICE is further expanding ACRIMe support for the Secure Communities initiative

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

As described above, ICE is combining ACRIMe and EID data via IIDS to enhance reporting throughout the ICE alien identification, apprehension and removal process. To effectuate this reporting, ICE is modifying ACRIMe to expand its user base within the agency, implementing new user

---

[4] NCIC codes are four-digit uniform offense classification codes whose literal translations best describe the offense(s) committed.

functionality in ACRIMe and EID, and updating IIDS to support enhanced reporting of ACRIMe and EID data. ICE is modifying both ACRIMe and EID to allow the assignment of ICE Levels to records about aliens in IAQs (in ACRIMe) and in booking records (in EID/EABM). This change supports ICE's implementation of and ability to report on its new enforcement priorities, which are focused on the removal of criminal aliens with a significant criminal history.

IIDS will receive additional data from EID and ACRIMe to support improved reporting that will reflect the implementation of new ICE enforcement priorities based on an alien's criminal history. IIDS will ingest ICE Level data in IAQs from ACRIMe and arrest and removal records from EID. Criminal history information from EID is also being included in IIDS. With this change, there is a privacy risk that PII may be over-proliferated by its duplication in multiple systems. In this case, ICE's reporting needs (i.e., to provide reporting that can be used internally and externally to effectively evaluate the implementation of ICE's enforcement priorities) cannot be served by existing reporting capabilities in either ACRIMe or EID because the data must be matched together to produce the analysis and statistics that are required by ICE and external parties. The duplication of limited data from ACRIMe and EID into a repository such as IIDS is an appropriate and necessary solution to this agency requirement. The privacy risks associated with this data duplication are minimized by the fact that only the necessary data fields from these systems are replicated in IIDS for reporting purposes, and the fact that queries are statistical in nature and not based on a particular person's case. Additionally, the ETL process filters the ACRIMe IAQ data to prevent IAQs for personnel security and special security event purposes from being included in IIDS, since those records are not part of the necessary reporting described in this PIA update. Finally, user access to IIDS is limited to only ICE employees with an established need to know and who are responsible for generating operational, senior management, and executive level statistical and performance reports. There is an additional privacy risk that the aggregated ACRIMe and EID data reported via IIDS may be incorrectly matched from the two systems. This risk is mitigated by the fact that, as previously stated, the information generated via IIDS is only statistical in nature and does not pertain to individuals' specific cases. If in reviewing statistics, ICE officers and agents want to drill further into a specific case, they must return to the source system(s) when making any enforcement or eligibility determinations.

In ACRIMe, the user will manually select the ICE Level from a drop-down menu (i.e., Level 1, 2, 3 or Not Applicable) during the processing of an IAQ, based on criminal history information already available to the user in ACRIMe from various government sources. There is a privacy risk that ICE Levels may be inaccurately associated with the subject of an IAQ because the users are manually selecting the ICE Level and could make an error. This risk is mitigated by user training describing the application of ICE Levels within ACRIMe using the ICE Level Mapping, which is keyed off of objective criminal history information (i.e., the NCIC code). This risk is further mitigated by leveraging the knowledge and experience of ACRIMe users who are trained to exercise judgment while reviewing and cross-checking information from multiple databases. This risk is also temporary in nature because ICE plans to automate the ICE Level calculation in ACRIMe in the future by incorporating ICE Level Mapping business rules that will be enforced by the system. This improvement will minimize the possibility of user error in identifying the correct ICE Level based on available criminal history data. Before deploying this new feature, ICE will publish an update to the ACRIMe PIA.

The expanded ACRIMe user population and the ability of the system to "refresh" an IAR in process with any new information allows ICE to more efficiently process the increasing number of IAQs

it receives. With new ACRIMe users there remains a risk of unauthorized use or disclosure of information contained in ACRIMe. This risk is mitigated by user training, user auditing, the maintenance of secure passwords, and the practice of operational and informational security. Individuals who are found to have accessed or used the ACRIMe system in an unauthorized manner will be disciplined in accordance with ICE policy. Additionally, ACRIMe users return a limited amount of data in IARs that is narrowly tailored to information that is useful to the law enforcement purpose for which the data was requested.

In EID, the ICE Level is system-generated based on business rules applied to the criminal history information that is now manually entered by the EID user (from government sources such as NCIC and TECS). These business rules are based on the ICE Level Mapping, which will help to ensure that the ICE Levels in ACRIMe and EID will be assigned consistently. The ICE Level Mapping has undergone several layers of review, and change management procedures have been put in place in order to address any updates or modifications to the ICE Level Mapping based on changes in law and/or policy. With this system modification, there is a privacy risk that criminal history information may be inaccurately entered and/or associated with the individual in EID. This risk is mitigated by primarily using the FBI number obtained from the fingerprint check conducted at the time of ICE arrest to query and retrieve criminal history information from NCIC.[5] Because the FBI number correlates to a biometric that identifies an individual, using the FBI number minimizes the risk that ICE will associate criminal history information with the wrong individual because of a same or similar name. This risk is also mitigated through training and guidance disseminated to EID users detailing the changes made to EABM and the criminal history information required to be entered (if available).

EID information is also subjected to data quality review processes such as field-level checks to ensure a minimum level of quality and completeness to detect employee errors and make appropriate corrections. If inaccurate data is discovered in EID, the system is updated with the correct information. Because EID relies on a central dataset rather than separate datasets for each ENFORCE application (e.g., EABM or EARM), the user need only correct the data in a single ENFORCE application to ensure the data is corrected throughout EID. There is an additional risk that ICE Levels generated in EABM for the crime(s) entered for subjects of an encounter may be inaccurate. This risk is mitigated by automating the ICE Level calculation based on ICE defined and approved business rules that directly map all NCIC codes to an ICE Level (i.e., the ICE Level Mapping).

When law enforcement agencies rely on criminal history information to make decisions about enforcement actions, there is a risk that the underlying criminal history information may be incomplete, inaccurate, or untimely for various reasons (e.g., final disposition missing, conviction overturned on appeal, etc.). ICE relies on criminal history information from the FBI, obtained via an NCIC query, and uses it to assign ICE Levels to individuals. If the underlying criminal history information is inaccurate, this may result in an incorrect ICE Level being assigned to an individual, which could result in incorrect prioritization of a case, the issuance of a detainer, or an arrest and initiation of removal proceedings. This risk is mitigated by the fact that ICE gathers and uses data from multiple sources of information, in conjunction with criminal history information, when deciding whether to take enforcement action against an individual, such as arrest or issuance of a detainer. ACRIMe and EID users are trained to exercise

---

[5] The fingerprint check occurs in the FBI Integrated Automated Fingerprint Identification System (IAFIS) as part of the Interoperability process.

judgment while reviewing and cross-checking information from multiple databases to ensure that enforcement actions are not taken without adequate legal grounds. This risk is also mitigated by the fact that ICE Levels are used internally for prioritization purposes only, and not to determine an individual's eligibility for removal. To remove an individual on the basis of a criminal conviction, ICE must obtain copies of the actual conviction documents, which would bring to light any errors in the criminal history record. The risk is further mitigated by the fact that immigration proceedings are an adversarial process in which the individual may challenge and present evidence contradicting the underlying grounds for removal, i.e., the criminal conviction information presented by ICE.

Uses of the System and the Information

Criminal history information in ACRIMe and EID will be used by individual ICE employees and the EID system itself, respectively, to identify the appropriate ICE Level for a particular alien according to the ICE Level Mapping. ICE law enforcement personnel will use the ICE Levels to prioritize their enforcement activities, i.e., the identification, arrest, apprehension, and removal of aliens. ICE Levels and criminal history information exported to IIDS will be used to evaluate the alignment of ICE enforcement activities with ICE's stated enforcement priorities, to assess the adequacy of resources, to generate internal reports for budgetary and other management purposes, and to meet external reporting requirements and requests to Congress, the news media, and the public.

Training, user auditing, access controls, and other standard system security controls, and the threat of disciplinary action or prosecution all mitigate the risk that the information in these systems will not be used in accordance with these stated purposes.

Retention

There are no changes to the retention periods described in the original ACRIMe and EID PIAs. Information extracted from ACRIMe and EID used for reporting via IIDS is retained in IIDS for the appropriate time periods, consistent with the ACRIMe and EID retention periods.

Internal Sharing and Disclosure

There are no changes to the internal sharing and disclosures described in the original ACRIMe and EID PIAs.

External Sharing and Disclosure

There is a risk that ICE Levels will be inaccurately associated with the subject of an IAQ. This risk is mitigated by user training describing the application of ICE Levels within ACRIMe, the ICE Level Mapping, and the importance of making accurate ICE Level determinations. There is also a risk of improper dissemination and compromise of information when returned to the criminal justice agency, the loss of which could present harm to an individual. Requesting criminal justice agency personnel are trained law enforcement officers and investigators responsible for securing and safeguarding information returned in an IAR appropriately, which mitigates this risk. Additionally, the information contained in an IAR is limited to the information provided by the requesting agency in the IAQ and an immigration status and ICE Level determination.

Notice

There are no changes to the notice procedures described in the original ACRIMe and EID PIAs.

Individual Access, Redress, and Correction

There are no changes to the access, redress, and correction procedures described in the ACRIMe and EID PIAs. These procedures are also described in the DHS/ICE-007 LESC ACRIMe system of records notice (SORN) (75 FR 8377, February 24, 2010) and DHS/ICE-011 Immigration and Enforcement Operational Records (ENFORCE) SORN (75 FR 23274, May 3, 2010).

Technical Access and Security

There are no changes to the technical access and security as described in the original ACRIMe and EID PIAs.

Technology

No technology is used that might raise privacy concerns.

Responsible Official

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security