Privacy Impact Assessment Update
for the

Enforcement Integrated Database (EID)

Prosecutions Module (PM), Electronic Removal Management Portal (eRMP), Operations Management Module (OM²), Law Enforcement Notification System (LENS), and Compliance Assistance Reporting Terminal (CART)

DHS/ICE/PIA-015(i)

December 3, 2018

Contact Point
Nathalie R. Asher
Acting Executive Associate Director
Enforcement and Removal Operations
U.S. Immigration and Customs Enforcement
(202) 732-3000

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Enforcement Integrated Database (EID) is a Department of Homeland Security (DHS) shared common database repository for several DHS law enforcement and homeland security applications. EID is owned and operated by U.S. Immigration and Customs Enforcement (ICE). It 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, U.S. Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS), components within DHS. DHS personnel access the data in EID using the ENFORCE suite of software applications, such as the ENFORCE Alien Removal Module (EARM). EARM supports ICE's processing and removal of aliens from the United States. The Privacy Impact Assessment (PIA) for EID was published in January 2010 and was last updated in January 2016.[1] ICE is updating this PIA to reflect changes to information that EID collects and stores, new uses of EID information, and enhanced sharing of EID data. The specific changes to the system are outlined in the "Overview" section below.

Overview

EID and the ENFORCE applications are used by personnel in the ICE Office of Homeland Security Investigations (HSI) and the Office of Enforcement and Removal Operations (ERO) to support ICE's arrest, detention, processing, and removal of aliens from the United States. This PIA update describes the following changes to EID and the ENFORCE applications:

1. Deployment of the Prosecutions Module used to support the ERO Criminal Alien Program;
2. Deployment of the Electronic Removal Management Portal (eRMP) used to support the ERO Removal Division and field offices;
3. Deployment of the Operations Management Module (OM²) used to support the ERO National Fugitive Operations Program;
4. Enhancements to the notifications sent by ICE's Law Enforcement Notification System (LENS); and
5. ICE's intention to procure and implement the Compliance Assistance Reporting Terminal (CART).

The following sections describe these changes in more detail.

[1] *See* DHS/ICE/PIA–015 Enforcement Integrated Database (EID) PIA and subsequent updates at http://www.dhs.gov/privacy.

Prosecutions Module (PM)

ICE developed the Prosecutions Module to track the status of aliens' criminal cases as they move through the judicial system. With this module, the ERO Criminal Alien Program (CAP)[2] manages an alien's case in a centralized manner. Under CAP, ERO officers are tasked with the identification and arrest of removable aliens who are incarcerated within federal, state and local prisons and jails, as well as at-large criminal aliens that have circumvented identification. It is incumbent upon ICE to ensure that all efforts are made to identify, arrest, and remove from the United States individuals who ICE has deemed a high priority by processing the alien expeditiously and securing a final order of removal for an incarcerated alien before the alien is released to ICE custody. The identification and processing of incarcerated criminal aliens before release from criminal custody reduces the time they spend in ICE custody and reduces the overall cost to the Federal Government. Additionally, integral to the effective execution of the program is the aggressive prosecution of criminal offenders who meet the criteria for criminal prosecution (e.g., a criminal offense under 8 U.S.C. § 1326 – Illegal Reentry). These aliens include: (1) those who have been arrested by a Law Enforcement Agency (LEA) and are incarcerated in federal, state, and local prisons and jails; (2) those who are in ICE custody; or (3) those who have otherwise been located by ERO officers.[3]

The Prosecutions Module allows ERO officers to create, approve, track, and report on criminal prosecutions of removable aliens in the officers designated Areas of Responsibility (AOR) in a more efficient manner. ERO officers can access the Prosecutions Module either directly from the EARM Homepage or independently using a web address. Regardless of which method the user chooses to access the Prosecutions Module, ICE ensures appropriate access by using 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.

To create a prosecution case, there must be an existing record in EARM for the alien.[4] Once ERO officers create a prosecution case, information related to the officer's investigation can be recorded and tracked. In addition, the officer can actively manage the case through the module by linking it to its associated administrative case.[5] Tracking the criminal alien's case enables ERO to

[2] For more information about the ERO Criminal Alien Program, please visit https://www.ice.gov/criminal-alien-program.
[3] In cases in which ERO knows where an alien is located (via visual or other means of confirmation), and the alien meets the criteria for criminal prosecution, ERO may elect to request a criminal arrest warrant from a magistrate judge showing that the alien is in clear violation of U.S. criminal law.
[4] An alien may have a record in EARM for a number of reasons. For example, ICE may be processing the alien for removal due to an administrative violation of the Immigration and Nationality Act (INA).
[5] An administrative arrest is based on a violation of U.S. immigration law, whereas, a criminal arrest is based on a

continue with the administrative removal process regardless of whether the Assistant United States Attorney (AUSA) declines to prosecute or the outcome of the criminal case results in an acquittal or a "not guilty" verdict.[6]

In a typical scenario, an ERO CAP officer will create a new prosecution case in the Prosecutions Module when he or she believes there is sufficient evidence to charge an alien with a criminal offense. Once the case is created, the officer will input any relevant information and present the case to a designated AUSA.[7] If the AUSA decides to prosecute the criminal case, the ERO officer will record all relevant case information (i.e., criminal offenses, date of case) and case proceedings, including case updates, into the prosecution record. Upon the conclusion of the criminal case, the ERO officer will select and submit the prosecution case to the appropriate supervisor within their AOR for approval.

Once the ERO officer submits the prosecution case for approval, the Prosecutions Module will automatically generate an email containing the name of the submitting officer, the date, the EARM case number, and the subject's Alien Registration Number (A-number), notifying the supervisor that the case is ready for review. Next, the supervisor reviews the case and either approves it or returns it for further updates. In either instance, the supervisor is able to provide comments to allow the officer to either revise and re-submit the case or receive other supervisory feedback related to the approved request. Upon final review and approval, the prosecution case will then be recorded as "Approved" and the prosecution's case record considered closed.

Alternatively, if the AUSA declines the prosecution case presented by the ERO officer, the ERO officer indicates that the AUSA declined to prosecute the case and records the reason for the declination. Cases declined for prosecution are not submitted to the supervisor for approval but are recorded as "Completed" (i.e., closed) and tracked on statistical reports. Regardless of the outcome of the prosecution case, the Prosecutions Module allows CAP to manage the lifecycle of criminal prosecutions in an effort to coordinate and expedite the removal of aliens from the United States.

Electronic Removal Management Portal (eRMP)

ICE recently developed the Electronic Removal Management Portal (eRMP) as a case management system to track aliens' custody status as they move through the Post Order Custody Review (POCR) process. By law, aliens detained under a final order of removal who are not

violation of U.S. criminal law, which is federally prosecuted by the U.S. Attorney's Office (USAO).

[6] Criminal convictions are not the only qualifying factor for removal. In accordance with the INA, certain aliens are removable from the U.S. The administrative (removal) process will continue regardless of the criminal case outcome, aside from the granting of a Stay of Removal or a benefit. ERO officers will work to confirm removability and, absent other legal impediments, remove the alien from the U.S. in accordance with all laws and regulations.

[7] Case presentation is conducted in accordance with the local operating procedure for the prosecutions programs developed by each ERO office, which establishes the appropriate notification procedures. For example, case presentation can be made by email, in-person file review, or by phone.

removed within the ninety-day removal period must go through the POCR process to ensure continued detention is justified and in compliance with governing statues, regulations, and policies.[8] In some cases, ICE may continue detention beyond the ninety-day removal period for a variety of reasons, including but not limited to: delays in securing travel documents, lack of diplomatic relations with the alien's country of origin, or legal proceedings triggered by the alien's legal representative. When ERO is unable to execute final orders of removal of detained aliens within the removal period, it must complete several key POCR steps by day ninety of the alien's detention. This process must be repeated every ninety days thereafter so long as the alien remains in custody and/or the case's standing removal order has not been executed.

Before ICE created eRMP, ERO officers used various manual paper-based processes to manage the functions related to the POCR process, creating processing delays and data integrity issues. eRMP is a time-sensitive module running on a "POCR clock," which runs daily and requires ERO officers to meet milestones and accomplish actions at precise times throughout the POCR case lifecycle. For example, day one (1) of the POCR clock begins once the final order of removal is issued and tracks the activities and other functions related to the removal of detained aliens (e.g., securing travel documents, legal proceedings) throughout the ninety-day removal period and continues until the execution of the officer's final determination. In addition, the POCR clock will trigger an email alert, sent to the assigned officer, for milestones that require immediate action. Finally, ERO officers can view and check the status of all active and closed cases for detainees in their AORs and obtain a snapshot of their custody status during the POCR process, provide custody recommendations, and record decisions.

ERO officers can access eRMP from the EARM Homepage, or independently using a web address. Similar to the Prosecutions Module, ICE ensures appropriate access by using SSO to validate ICE users with PIV-card authentication. To create a POCR record in eRMP and begin the POCR process, an EARM case record must already exist for the detainee. In a typical transaction, an ERO officer will create a POCR record once the alien is in ICE custody and a final order of removal has been issued. An ERO officer then enters the detainee's A-number into eRMP to create a detainee's POCR record. During the POCR process, ERO officers are required to review the entire case and submit a recommendation (known as a Decision Letter) to the appropriate supervisor to either continue the alien's detention or release the alien from ICE custody. The Decision Letter is generated in eRMP and must be reviewed and approved by a Field Office supervisor. Once a supervisor makes the final determination and signs the Decision Letter, the letter is uploaded into eRMP, a hard copy is placed in the detainee's file, and the ERO officer must then provide the signed Decision Letter to the alien, either by certified mail or in person. With this

[8] By statute, when an alien is ordered removed, federal agencies must remove the alien from the United States within a ninety-day period. *See* 8 U.S.C. 1231. In addition, the Supreme Court ruled in *Zadvydas v. Davis* (533 U.S. 678) that unlimited detention beyond the ninety-day period is not reasonable. Federal agencies must justify why aliens are detained beyond the ninety-day removal period.

module, the ERO Removal Division can ensure that POCRs are being conducted in a timely manner and cases are tracked through their completion.

Operations Management Module (OM²)

ICE developed the Operations Management Module (OM²) to assist the ERO National Fugitive Operations Program (NFOP) to identify, locate, and arrest persons of interest or fugitive aliens sought by ICE. The NFOP leverages the personnel at the National Criminal Analysis and Targeting Center (NCATC)[9] and Fugitive Operations Teams (FOT) to achieve this objective.[10] Before ICE created OM², ERO used the Fugitive Case Management System (FCMS).[11] FCMS has since been retired and its functionality has been incorporated into OM², a module within EARM. With this module, ICE agents and officers can generate and track leads (e.g., addresses and phone numbers), manage mission operations, track activities (e.g., arrests by team, target details) and link targets with specific operations.

OM² is only accessible by logging into EARM and requires that the alien already has an active EARM record. In a typical transaction, ICE receives information from a variety of sources to generate lead information on fugitive aliens. Such sources include: public or government records; information from federal and state correctional facilities that may locate a fugitive alien in jail or prison; or information from commercial sources. OM² users (either at the NCATC or members of FOTs) can either manually enter leads one at a time or in bulk, which are then linked to the fugitive alien's existing record using the target's A-number.

Once the lead information is uploaded into the OM² database, these new leads are assigned to the appropriate FOT to investigate, and when possible, arrest the target alien. As part of the investigative process, ERO officers will evaluate the lead information, manually compare other sources of information such as leads from commercial sources against Federal Government databases, validate information for accuracy, and document and update OM² as the investigation progresses. If the fugitive is arrested, ERO updates the fugitive alien's status in OM² to reflect that he/she is now in ICE custody. OM² allows ICE agents and officers to develop and track new leads, associate multiple leads with a target(s) and/or ongoing operation(s), and manage and record investigative and arrest activities.

Law Enforcement Notification System (LENS)

ICE developed the LENS interface within the EARM application to send notifications to other state and local law enforcement agencies via the National Law Enforcement Notification

[9] The NCATC serves as a national enforcement operations center for the ERO Targeting Operations Division (TOD), providing critical information to ICE law enforcement officers in the field and headquarters components.
[10] For more information about NFOP, please visit: https://www.ice.gov/fugitive-operations.
[11] For more information about FCMS, see DHS/ICE/PIA-009, at https://www.dhs.gov/publication/dhsicepia-009-fugitive-case-management-system-fcms.

System (NLETS).[12] NLETS is a network used by federal, state, and local law enforcement agencies for the exchange of law enforcement, criminal justice, and public safety-related information.[13] This information allows state and local law enforcement agencies to identify individuals who are being released by ICE into their respective jurisdictions. Currently, a LENS notification message is triggered when an alien convicted of a violent or serious crime (e.g., homicide, sexual assault, aggravated assault, or robbery) is released from ICE custody.[14] If the criminal alien indicates that he plans to reside in a different state than the one to which he is released, ICE will also automatically notify the law enforcement agency of the state of intended residence.

ICE only shares the following biographic date elements in the LENS notification message with law enforcement agencies: name, alias, date of birth (DOB), address of the alien's residence, country of citizenship, A-number, and other identifying law enforcement numbers (e.g., state identification number, FBI number, fingerprint number). With this information, the respective law enforcement agency may conduct its own inquiry in the Federal Bureau of Investigation's (FBI's) National Crime Information Center (NCIC) database to view the alien's criminal history. These notifications are for situational awareness only. They neither direct nor require law enforcement agencies to take action, but rather help inform agencies that have an interest in an alien in connection with a pending investigation or prosecution, for parole or other forms of supervision, or for public or officer safety purposes. With this PIA Update, ICE is informing the public that a LENS notification message will now be triggered and shared with law enforcement agencies for aliens on the National Sex Offender Registry (NSOR) when they are released from ICE custody into their respective jurisdictions.

A new data field within EARM will allow ERO officers to indicate whether the alien is in the NSOR. At the time a detainee is released from ICE custody, ERO officers are required to query the FBI's NCIC database to determine if there is a NSOR alert in the system. If there is a NSOR alert, ERO officers must verbally notify the detainee of his or her sex offender status and responsibilities (e.g., registering with local law enforcement and retaining written proof of registration) and indicate the alien's NSOR status in EARM, thereby triggering the LENS notification message. The information contained within the LENS notification message will remain the same, but the new data field will now allow ICE to automatically send a LENS notification to the law enforcement agency where the alien intends to reside.

Compliance Assistance Reporting Terminal (CART)

ICE is developing a capability known as the Compliance Assistance Reporting Terminal (CART) to automate the check-in process for aliens with reporting requirements on the non-

[12]For more information LENS please see EID PIA and EID PIA Update at http://www.dhs.gov/privacy.
[13] For more information on NLETS, see http://www.nlets.org.
[14] See EID PIA Update Appendix for a list of crimes that trigger automated notifications at http://www.dhs.gov/privacy.

detained docket. The non-detained docket is comprised of aliens who have been released from detention with final deportation orders or are awaiting final court decisions on their immigration status.[15] The current non-detained reporting process requires aliens to check in at regular intervals to report any changes to their status (e.g., address, contact information) and to ensure compliance with the terms of release. The check-in process is generally routine and repetitive in nature, and involves ERO officers conducting in-person interviews, placing a significant burden on ERO officers with little added value in return. CART is expected to reduce the time and resources ERO officers devote to managing the check-in process for these aliens and allow ERO Officers to focus on higher-risk cases, such as aliens who pose a threat to public safety and other enforcement priorities.

CART consists of both a stand-alone, self-service kiosk (similar in appearance to an ATM) and a system that permits ERO personnel to conduct CART enrollments, update information as necessary, manage daily CART activities (particularly secondary reviews), and run reports.

The CART Kiosk

The CART kiosk is a self-service kiosk used by selected aliens on the non-detained docket during the automated check-in process. The kiosk contains several features, such as a touchscreen display, camera for photo capture and testing of facial verification, fingerprint scanner, printer, and the capability to support multiple languages. These kiosks will be located inside ICE ERO field offices, such as a waiting room. CART will enable eligible aliens on the non-detained docket with Orders of Supervision (OSUP) or Orders of Recognizance[16] to check in with ERO using the kiosk rather than meeting with an ERO officer in person.

When an alien visits a CART kiosk, he or she will initiate the CART system and confirm that he or she is a CART enrollee by entering his or her A-number. The system will prompt the user to scan his or her fingerprints and will capture a photograph to confirm his or her identity for the identity verification process. The photograph captured and stored by CART is only used to confirm the identity of the alien who was using the kiosk at the time of check-in. The CART kiosk will query the fingerprints against DHS's Automated Biometric Identification System (IDENT)[17] database to verify the identity of the CART enrollee. The facial image will be sent and stored in both IDENT and EID.

---

[15] Aliens on the non-detained docket are still subject to removal under the Immigration and Nationality Act (INA), but are not subject to mandatory detention. These individuals are on the non-detained docket for a variety of reasons, such as they do not pose a risk to public safety, are a low flight risk, and/or there is a low risk that they will fail to comply with release requirements.

[16] An Order of Supervision (OSUP) and/or Recognizance exists when an alien is released from detention under prescribed reporting conditions after receiving a final order and because ICE was unable to effect deportation or removal during the period prescribed by law.

[17] The National Protection and Programs Directorate (NDDP)/Office of Biometric and Identity Management IDENT DHS/NPPD/PIA-002, can be found at http://www.dhs.gov/privacy.

The kiosk will conduct a biographic query against the FBI's Next Generation Identification System (NGI)[18] using the FBI Universal Control Number (UCN) stored in EID to search for any recent criminal history activity. The CART kiosk will never display an alien's criminal history on the screen itself.

The CART kiosk requires the enrollee to confirm and respond to a list of inquires related to the non-detained reporting check-in process. The system will ask the user to: (1) confirm his/her address and telephone number, which are maintained in EID; (2) indicate any future travel plans; and (3) indicate whether he/she wants to speak with a live ERO officer. The only PII that will appear on the screen are the alien's address and telephone number, which reflect the most recent data in EID. Lastly, certain changes to an enrollee's current profile or circumstance/status may trigger a Manual Secondary review conducted by an ERO officer.

The CART System

The CART system permits ERO offers to engage in the following activities:

- Enrollment of aliens to use the CART kiosk;
- Management of CART profiles;
- Tracking CART enrollees' check-ins;
- Receiving and addressing Manual Secondary Review notifications
- Creating and generating various CART reports;
- Allow ERO Officers to ensure compliance with the non-detained check-in process; and
- Storing and retrieving all CART-generated data.

Reason for the PIA Update

The PIA for EID was last updated in January 2016, and reflected the system at that time. The ENFORCE applications, used to access the data in EID, continue to be enhanced to support ICE's changing business and operational needs and the PIA is being updated to reflect those changes.

Privacy Impact Analysis

Authorities and Other Requirements

DHS has been authorized to collect information under 5 U.S.C. § 301; 8 U.S.C. § 1103; 8 U.S.C. § 1225(d)(3); 8 U.S.C. § 1226; 8 U.S.C. § 1324(b)(3); 8 U.S.C. § 1357(a); 8 U.S.C. §

[18] Integrated Automated Fingerprint Identification System/Next Generation Identification Biometric Interoperability, *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

1360(b); 8 U.S.C. §§ 1365a and 1365b; 19 U.S.C. § 1; and 19 U.S.C. §§ 1509 and 1589a. Additional authority is provided in 6 U.S.C. § 202; 8 U.S.C. §§ 1158, 1201, 1379, and 1732; and 19 U.S.C. §§ 2071, 1581-1583, and 1461; and the Immigration Reform and Immigrant Responsibility Act of 1996.

The DHS/ICE 011-Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN applies to the information collected and maintained by EID.[19] A system security plan for EARM has been completed, and the Authority to Operate (ATO) was authorized on July 21, 2016. The Authority to Operate (ATO) for EARM expires on July 21, 2019.

Records Retention Schedule

Records maintained in EID, including biographic and biometric information maintained in EID fall under Records Control Schedule DAA-0563-2013-0006.[20] This schedule maintains records regarding the identification, investigation, apprehension, and/or removal of aliens unlawfully entering or residing in the United States. Under this schedule, records are retained for 75 years from the end of the calendar year in which the data is gathered. This ensures that the records are kept for at least the lifetime of the individuals to whom they pertain because they document the arrest, detention, and possible removal of individuals from the United States. This includes fingerprint and photograph records collected using the EDDIE mobile device.

Characterization of the Information

As noted in the Overview, EID (and the applications that use it), 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. Enhancements have been made to the system to enable it to collect additional information to better assist ICE personnel with their immigration and law enforcement missions. The various categories of information collected, used, disseminated, and maintained will now include the following:

Prosecutions Module

Information related to an alien's criminal prosecution includes, for example:

- The date the case was created, the date the case was presented to the AUSA, and the corresponding judicial district;
- Status of the alien's criminal case (e.g.., accepted or declined by AUSA);

[19] DHS/ICE–011 Criminal Arrest Records and Immigration Enforcement Records (CARIER), 81 FR 72080 (Oct. 19, 2016). The CARIER SORN has replaced what was formerly known as the ENFORCE SORN.
[20] The retention schedule can be found here: https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-homeland-security/rg-0563.

- The presentation offense (e.g., fraud, re-entry after deportation), and other information pertaining to the alien's arrest, such as date of arrest, arrest violation, and case number;
- The officer's name, AOR, and Docket Control Office (DCO) to whom the case is assigned;
- Investigation and court proceeding notes related to the prosecution case; and
- Date of disposition; and judicial decision for each violation (i.e., convicted, dismissed), and when applicable, sentence term or supervised release term.

Electronic Removal Management Portal (eRMP)

Information related to a detainee's POCR process includes, for example:

- Information specifically related to the detainee's removal proceedings (e.g., whether travel documents have been secured, or whether there is a pending writ of Habeas Corpus);
- Contact information of federal employees and contractors involved in the POCR process, such as names, phone numbers and email addresses;
- Recommendations made by the POCR case officer;
- Medical/Disability and psychological conditions, concerns, professional diagnosis, and treatment plan;
- The name of agency and probation/parole officer;
- Disciplinary records and related information;
- Information obtained during subject interviews, such as the name of interviewing officer, and if applicable, the name of an interpreter; and
- Biographical history, such as detainee's potential residence, family members, education and employment history.

Operations Management Module (OM²)

Lead and activity information related to the tracking and apprehension of fugitive operations and aliens includes, for example:

- The address for the lead, and address type (e.g., home, permanent or temporary residence, commercial or work address(es));
- Phone numbers of targets associated with the lead;
- Name and AOR of officer who entered the lead;
- Source of the lead (Field, NCATC, or HQ);
- The officer who submitted the activity and the date on which the activity was submitted and occurred; and

- Information pertaining to the arrest, such as type of arrest (e.g., vehicle stop), activities (e.g., arrest closures), identification documents acquired by the arresting officer at the time of arrest, criminal/immigration violations, status of alien, and operation name (if applicable).

Law Enforcement Notification System (LENS)

- Information indicating whether the alien is in the NSOR will now be included within the LENS notification.

Compliance Assistance Reporting Terminal (CART)

- Biometric data (e.g., fingerprints, facial image) and other information already contained in EID will now be used during the non-detainee docket check-in process to verify the individual's identity and confirm compliance with the terms of his or her release.[21]
- New information related to the non-detained docket check-in process, such as CART enrollee profiles will be collected and maintained within the CART system.

Sources of Information

The modules identified in this PIA obtain information from similar sources, such as:

- ICE and other DHS and government systems that contain information about the alien as the result of immigration enforcement or other law enforcement encounters with the alien;
- Public or government records;
- Federal and state correctional facilities that may locate a fugitive alien in jail or prison;
- An alien's application for immigration benefits;
- Records of the alien's admission into the United States; and
- The alien him or herself at the time of arrest and/or placement into ICE custody, and from the ERO Officers during the arrest activities.

The following are examples of specific sources of the information collected, used, disseminated and maintained in EID:

Prosecutions Module (PM)

- Information related to an alien's criminal prosecution case is retrieved from the Public Access to Court Electronic Records (PACER) system, which is owned and maintained by the Administrative Offices of the U.S. Courts. PACER is an electronic access service that allows

[21] Biometric data provided by CART enrollees will not be stored in EID, but rather will only be used to verify the user's identity during the check-in process.

users to obtain case and docket information online from federal appellate, district, and bankruptcy courts.

- Information related to where an alien or inmate is being held or serving their sentence is retrieved from the Federal Bureau of Prisons (BOP) inmate information system (SENTRY)[22] and manually entered into the PM. SENTRY is a real-time information system consisting of various applications for processing sensitive but unclassified (SBU) inmate information.

Operations Management Module (OM²)

- ERO Field Officers manually inputting information based on their evaluation of leads and address information;
- Manual and batch checks against U.S. Postal Service commercially available data sets that update city and state information by zip code. These data sets do not contain PII.
- Commercial sources that provide relevant open source (i.e., publicly available) information about removable aliens. This open source data increases the probability of locating an alien for apprehension and removal. This data includes, but is not limited to, biographical information, criminal history, criminal case history, and vehicle information (including vehicle registration information).

Compliance Assistance Reporting Terminal (CART)

- NPPD/OBIM IDENT[23]
- DOJ/FBI NGI[24]

Privacy Risk: The system could contain inaccurate information, which could increase the likelihood of adverse action being taken against an individual based on incorrect information.

Mitigation: This risk is partially mitigated. Most of the information is collected directly from the individual, which increases the likelihood that it is accurate. For example, CART will leverage DHS's biometric database, IDENT, to verify the alien's identity and to ensure compliance with the terms of their release (e.g., address, travel, current criminal activity). Information provided by the alien is cross-checked against data in other ICE/government systems via biometrics to ensure correlation between identity and data and confirmed by ICE personnel.

In addition, ICE does not take any adverse action against individuals until it confirms the accuracy of the information. For example, ERO officers take actions to manually verify and validate lead and arrest information in other public and federal systems, such as running a check

[22] The Federal Bureau of Prisons (BOP) inmate information system (SENTRY), available at, https://www.bop.gov/foia/#tabs-4 OR https://www.bop.gov/foia/sentry.pdf.
[23] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System, *available at* http://www.dhs.gov/privacy.
[24] *See* Integrated Automated Fingerprint Identification System/Next Generation Identification Biometric Interoperability, *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments.

to confirm a new address belongs to a fugitive alien before performing surveillance, when they are investigating each case in OM².

Privacy Risk: There is a risk that the system(s) collects more information than is necessary for the purposes of the program.

Mitigation: This risk is partially mitigated. ICE collects only a limited amount of information about individuals that is narrowly tailored to effectively and efficiently carry out the purposes of the program. For example, ERO CAP uses the Prosecutions Module to track only criminal prosecutions; it does not contain information regarding aliens' immigration proceedings. Another example is the limited subset of information collected and used by CART. The information requested is specifically related to the check-in process for aliens on the non-detained docket to verify their identity and ensure compliance with the terms of their release (e.g. address, travel, current criminal activity), and the only new information collected will relate to the user's contact information.

Uses of the Information

The goal of the above enhancements is to allow ERO to manage and track the enforcement lifecycle in an efficient and centralized manner, and to provide oversight and facilitate logistical and operational support to twenty-four ERO field offices and division office teams (e.g., FOTs). The information contained in EID is used to identify, track, apprehend, detain, process, and remove aliens from the United States. The various modules and subsystems in EARM capture and report all required information related to enforcement and removal activities, and as a result, EID information is used to assist ERO personnel and officers with removal operations and tracking of removable aliens until the subjects depart from the United States. These activities use EID information to perform the following specific functions:

- Manage the lifecycle of criminal prosecutions in an effort to coordinate criminal prosecutions and/or later expedite the removal of criminal aliens from the country;
- Manage the detention and removal process for aliens that have been issued a final order of removal to ensure compliance with laws, regulations, and policies;
- Identify, track, locate, and arrest or otherwise take custody of fugitive aliens for detention and, if judged removable, to remove them from the country;
- Send message notifications to other state and local law enforcement agencies via NLETS when an alien convicted of a violent or serious crime (e.g., homicide, sexual assault, aggravated assault, or robbery) is released from ICE custody in that state; and
- Verify the identity of aliens on the non-detained docket and ensure compliance with the terms of their release.

Reporting

EID allows EARM modules and subsystems to generate standard and ad hoc reports based on the information entered into the system. In addition to generating case-related reports, EID information can be used to generate reports for statistical and performance-based purposes to further support the enforcement and removal processes and provide oversight. Examples of the various reports generated include the following:

- The Prosecutions Module generates reports that contain data on criminal arrests, indictments, convictions, and case information, and the reports may break down the information by category or type of violation.
- OM² generates activity and lead reports that contain biographical information about targets, information about activities recorded by officers, and a list of leads for targets and operations.
- CART reports are generated for management and auditing purposes. Management will have the ability to generate a report for a specific CART enrollee, and authorized users will have the ability to generate reports to evaluate the performance of the system.

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

Mitigation: The Prosecutions Module, eRMP, and OM² have limited access controls in which only authorized users with a need to know have access to the system and the PII contained within. Access roles are designated by the individual's position, which ensures that users are only granted access to the information necessary to perform their official duties. Regarding the Prosecutions Module and eRMP, users can access both modules directly using a web address. ICE ensures appropriate access by using SSO to validate ICE users with 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.

Privacy Risk: There is a risk that individuals will use the information in the system for purposes beyond what is described in this PIA.

Mitigation: Any ICE personnel who have accessed the system without authorization or who used the database in an inappropriate manner may be disciplined, which may include revoking access to the database, suspension, or termination of employment. User roles and access controls are incorporated that limit user capabilities so that only users with a need to know can access specific portions of the system. Users are barred from accessing certain information. For example, ERO officers can only access records for cases within their AOR, which restricts users from adding and editing cases outside their own AOR.

In addition, audit logs are reviewed by supervisors to ensure ERO's personnel proper use of the system (e.g., login times, records accessed, reports generated). For example, CART allows supervisors to generate reports and to ensure that ERO officers are using the CART application appropriately.

Privacy Risk: There is a risk that individuals other than eligible CART enrollees may access the CART kiosk.

Mitigation: This risk is mitigated. Only individuals who are on the non-detained docket are eligible for CART enrollment. In order for an alien to access a CART kiosk, an ERO officer must enroll the alien using the CART system. In addition, when an alien visits a CART kiosk, he or she must be able to provide and enter two discrete identifying pieces of information about him or herself: (1) the A-number; and (2) fingerprints to successfully confirm CART enrollment and initiate and complete the automated CART check-in process. Because the kiosks are located in public areas (e.g., waiting rooms at ERO field offices) where bystanders are in close proximity, the only sensitive personally identifiable information that will be visible are the individual's A-number, (which will be replaced by an asterisk as each digit is keyed in), and the alien's address and phone number. Lastly, after a short period of non-use, the individual's check-in session will end and all incomplete sessions will be reported to ERO personnel.

Notice

For CART, ERO officers will notify and explain the CART enrollment process to aliens who are on the non-detained docket and who meet the qualifications for the automated check-in process during an in-person interview with an ERO Officer. For LENS notifications, detainees in the NSOR file will be notified of their current status and responsibilities by the ERO officer at the time of their release from ICE custody. ICE provides general notice about the system and the information it maintains in the DHS/ICE/PIA-015 EID PIA[25] (January 14, 2010), this update, and the DHS/ICE-011 Criminal Alien Records and Immigration Enforcement Records (CARIER) System of Records Notice (SORN).

Privacy Risk: There is a risk that individuals may not be aware that their information may be contained within the system, and/or may not understand the notice provided.

Mitigation: This risk is partially mitigated. Aliens on the non-detained docket will be notified by an ERO ICE officer during the in-person interview that they are CART-eligible and will complete the check-in process by verifying their information using the CART kiosk. In some cases, ICE is not able to provide additional notice because the information is used for law enforcement purposes. Providing individuals with notice or the opportunity to consent to the agency's use of information would compromise the ability of the agencies to perform their

[25] DHS/ICE/PIA-015 Enforcement Integrated Database, available at www.dhs.gov/privacy.

missions and could put law enforcement officers at risk. Access to records could inform the subject of an actual or potential criminal/civil/regulatory violation and the record subject could impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension if he or she could access this information. Permitting access (or providing notice) could also disclose sensitive information that could be detrimental to homeland security.

Data Retention by the project

The original PIA for EID/EARM indicated that records were maintained in EID for 100 years. The records schedule for EID (referenced above) has since been updated, and all information entered into EARM is now retained in EID for 75 years from the end of the calendar year in which the information is gathered.

Information Sharing

There have been two changes to how data is shared outside DHS. First, LENS includes additional information contained within the message notification indicating whether the individual is in the NSOR file. Second, in accordance with Routine Use A in the DHS/ICE-011 CARIER SORN, CAP shares information from the Prosecutions Module regarding aliens who have violated U.S. criminal laws with the Department of Justice (DOJ), including Offices of the United States Attorneys, to facilitate criminal prosecutions for fugitive aliens.

Privacy Risk: There is a risk that data will be shared with external parties who do not have a need to know.

Mitigation: This risk is mitigated because ICE only shares the minimum amount of information necessary with recipients who have a need to know the information, and the sharing is authorized under applicable routine uses. For example, under Routine Use A of the CARIER SORN, CAP officers only share investigative information with AUSAs regarding the alien's criminal offense. Another example is the additional information contained within the LENS notification. At the time of a detainee's release from ICE custody, ERO officers are required to query FBI's NCIC to determine if there is a NSOR alert in the system to ensure the information shared with law enforcement entities reflects the detainee's current status on the NSOR. In addition, LENS information is shared with law enforcement entities that have a need to know and is restricted to aliens being released from ICE custody into their respective jurisdictions. Finally, sharing is authorized under applicable Routine Use Z of the CARIER SORN for the purpose of providing notice of an individual's release from DHS custody.

Redress

The right to request 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 No. 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."[26] 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.[27]

As a result of Executive Order 13768, DHS's "Mixed Systems Policy"[28] was rescinded by the DHS Privacy Office in its Privacy Policy Guidance Memorandum 2017-01 (April 25, 2017).[29] This changes the ability of aliens to access and correct their record maintained in a system of records at DHS, such as EARM or ICM. Individuals not covered by the Privacy Act or the Judicial Redress Act may request access to their records by filing a Freedom of Information Act (FOIA) request. The DHS Privacy Policy Guidance Memorandum 2017-01 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 DHS personnel, and can create the risk of errors made by DHS and its personnel. To that end, the Privacy Division in the ICE Office of Information Governance & Privacy accepts records amendment requests from individuals not covered by the Privacy Act of 1974. Individuals can

[26] Executive Order No. 13768 *Enhancing Public Safety in the Interior of the United States* (January 25, 2017), https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[27] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017, 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.

[28] 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 U.S. citizens and lawful permanent residents, and non-U.S. citizens and non-legal permanent residents). Memorandum Number 2007-1, DHS Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.

[29] 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.

either submit these requests by email to ICEPrivacy@ice.dhs.gov or by mail to the following address:

ICE Information Governance & Privacy Office
ATTN: Privacy Division
500 12th Street SW, Mail Stop 5004
Washington, DC 20536.

Auditing and Accountability

EID modules outlined in this PIA follow the same auditing and accountability procedures described in the EID PIA and subsequent PIA updates. For example, system administrators employ access controls to make sure only authorized users can access the data in the system. Additionally, role-based access is used so that users only have access to the information necessary for their positions. Certain user groups may only have "read only" access, while other groups have "read, write, edit privileges." This is based on the user's job responsibilities, implemented by system administrators. Individuals who no longer require access have their credential removed from the system.

Finally, the system and modules identified here maintain audit logs of user activity to monitor unusual behavior in the system. Audit logs will track when individuals are logged into the system. If the system administrators notice that anyone has used the system in violation of ICE policy, the user will be disciplined.

Responsible Official

Jordan Holz
Acting Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

[Signed copy complete and on file with the DHS Privacy Office]

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security