Privacy Impact Assessment
for the

Enforcement Integrated Database (EID)

January 14, 2010

Contact Point
James Dinkins
Director, Office of 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 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 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 U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), both agencies within DHS. The majority of records in EID are predicated on ongoing DHS law enforcement activity. This privacy impact assessment (PIA) is being completed to provide additional notice of the existence of the EID and the applications that access EID, and to publicly document the privacy protections that are in place for the system.

Overview

EID is a common database repository owned and operated by U.S. Immigration and Customs Enforcement (ICE) that supports the law enforcement activities of certain DHS components. EID is the repository for all records created, updated, and accessed by a number of software applications collectively referred to as the "ENFORCE applications." EID and the ENFORCE applications capture and maintain information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and law enforcement investigations and operations conducted by ICE and U.S. Customs and Border Protection's (CBP) Office of Border Patrol and Office of Field Operations. An event-based record for each encounter is created in EID, but the system provides users the capability to access a person-centric view of the data as well through accessing data within the ENFORCE applications. Users can also print reports, notices, and other documents containing EID data, which are typically retained in criminal and administrative investigative case files and in Alien Files (A-Files). Immigration related forms generated by the system are also sent to courts and other agencies to support the advancement and adjudication of DHS and Department of Justice immigration cases. Forms and data may also be provided to the criminal courts of the United States.

This PIA describes the EID and the ENFORCE applications that use the EID as a data-store to support DHS law enforcement processes and workflows, especially those related to the enforcement of immigration laws. As an alleged immigration violator (i.e., subject) moves through the enforcement process, DHS personnel create, modify, and access the data stored in the EID's central data repository using different ENFORCE applications. Which ENFORCE application is used depends on the particular phase of the immigration enforcement process a subject is in (arrest, booking, detention, or removal). For example, the ENFORCE Apprehension Booking Module is used to process arrests during the immigration process, but also supports ICE's arrest and booking of subjects for violations of U.S. customs laws and other federal criminal laws. Each ENFORCE application is described below.[1]

[1] In addition to the applications described in this PIA, CBP is developing an application called SIGMA, which will provide CBP personnel with a modernized user interface to EID. SIGMA will provide an alternate way for CBP

ENFORCE Apprehension Booking Module (EABM)

EABM is an event-based application that integrates and supports law enforcement arrest and booking functions including apprehension processing, fingerprint and photographic identification, recording of allegations and charges, preparation and printing of appropriate forms, and interfaces with other applications. ICE and CBP use the EABM to track the apprehension of individuals (both non-U.S. Citizens and U.S. Citizens) who have been arrested by ICE or CBP for violating U.S. customs and other federal criminal laws, and/or violations of administrative or criminal provisions of the Immigration and Nationality Act (Title 8, United States Code). The EABM also allows for the creation of records about individuals who are either the subject of ongoing criminal investigations or who are amenable[2] to removal proceedings but are not in the custody of DHS. These "subject" records may be used as part of an ongoing investigation and sometimes are used to place immigration detainers[3] when DHS is seeking custody of an alien who is already in the custody of another federal, state, or local law enforcement agency. EABM also receives information from the U.S. Visitor and Immigration Status Indicator Technology (US-VISIT) program's IDENT biometric database, such as the subject's Fingerprint Identification Number and photographs.[4] EID uses the Fingerprint Identification Number to identify EID records that may be about the same person, enabling the user to determine whether to link the records. EABM is also used to record biographical information of those prisoners that ICE holds for the U.S. Marshals Service under an interagency agreement.

ENFORCE Alien Detention Module (EADM)

EADM is an application that allows the ICE Office of Detention and Removal Operations (DRO) to track the detention of subjects in ICE custody charged with violations of the Immigration and Nationality Act. EADM contains "subject records" about aliens who are in or about to begin immigration proceedings to remove them from the United States based on their immigration status. EADM uses data collected through EABM at the time of a subject's arrest and booking. EADM is also integrated with the ENFORCE Alien Removal Module, described below. EADM is also used to track prisoners that ICE detains for the U.S. Marshals Service under an agreement with ICE. When a subject is released from detention, EADM is updated to indicate the date of release and release type (e.g., release on bond).

---

personnel who are current ENFORCE applications users to access and write to EID. SIGMA details will be addressed in a separate PIA.

[2] The term "amenable" in this context means "liable to be brought to account" when an alien appears to be in violation of the Immigration and Nationality Act. The term "amenable" is used to distinguish it from the term "eligible," which is used when DHS (specifically, U.S. Citizenship and Immigration Services) can issue a benefit to an alien.

[3] DHS employees designated as immigration officers/agents (as defined by the Immigration and Nationality Act Section 101(a)(18)) have legal authority to issue an Immigration Detainer-Notice of Action to any other Federal, State, or local law enforcement agency. The Immigration Detainer advises that agency that DHS seeks custody of an alien presently in the custody of that agency for the purpose of arresting and removing the alien from the U.S. The detainer is a request that such agency advise DHS before the alien is released from custody so that DHS can arrange to assume custody of the alien.

[4] The Fingerprint Identification Number is a number assigned by US-VISIT to each unique set of fingerprints in the IDENT database. *See* DHS/USVISIT-0012 DHS Automated Biometric Identification System (IDENT), 72 FR 31080, June 5, 2007.

ENFORCE Alien Removal Module (EARM)

EARM is an application that supports ICE's processing and removal of aliens from the United States. ICE DRO personnel use EARM primarily as a case management tool to track the status of alien removal proceedings. EARM provides personal identifiers, photographs, and details of removal case proceedings to aid DRO in carrying out the removal of aliens from the United States. EARM is currently in its first phase of release; future releases will provide additional capabilities in support of detention and removal business processes and will interface with internal and external enforcement systems to support alien removals, detentions, and alternative-to-detention program activities. Subject arrest and booking information collected through EABM is accessed and used by DRO personnel during the detention and removal processes through EADM and EARM. Using EARM, a user may be able to view the entire detention history of a subject in ICE custody (all prior or current detention record data captured in the EID). While EABM, EADM, and EARM each allow for different user access privileges and support different stages of the law enforcement process, they all use and access a centralized set of data on the individual which enhances data accuracy and currency. EARM and EADM replaced the Deportable Alien Control System (DACS), a legacy Immigration and Naturalization Service system that has been retired.

In conjunction with case management, DHS captures fingerprints and photographs in this process through the Enforcement Automated Biometric Identification System (WebIDENT) and Mobile IDENT. This information is maintained in IDENT. All case management information related to this information is maintained in EID.

Enforcement Automated Biometric Identification System (WebIDENT)

WebIDENT is an application that is used to capture fingerprints and photographs during the arrest and booking of subjects by ICE, CBP, and U.S. Coast Guard law enforcement personnel. WebIDENT submits the fingerprints and photographs to the US-VISIT IDENT biometric database and submits fingerprints to the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS) database for storage and for fingerprint-based criminal records checks.[5] WebIDENT receives and displays the results of fingerprint searches against IDENT and IAFIS and has the ability to retrieve additional information from U.S. Department of State (DOS) databases pertaining to visa issuance and passport data based off of the fingerprint match. For arrests entered through EABM, IDENT sends WebIDENT the Fingerprint Identification Number for the subject, which is then stored in the subject's EID record.

Mobile IDENT

Mobile IDENT is a Web interface that enables DHS officers/agents to perform fingerprint checks through WebIDENT from the field using a laptop computer and portable fingerprint scanner with a virtual private network (VPN) connection. The purpose of Mobile IDENT is to improve processing times when DHS officers/agents conduct apprehensions in the field. It allows DHS personnel to determine a subject's immigration status in the field without driving long distances to DHS offices, thereby improving

[5] *See* Justice/FBI-009 Fingerprint Identification Records System (FIRS) System of Records Notice, 64 FR 52347, Sept. 28, 1999.

processing times and enabling appropriate releases onsite. For example, the U.S. Coast Guard uses Mobile IDENT to access WebIDENT remotely in order to verify the identity of individuals encountered on vessels at sea using fingerprints or photographs. Mobile IDENT also allows DHS officers/agents to modify, read, and create alien booking records, including fingerprint and/or photographic data, in EABM and WebIDENT, while storing no data on the device itself. Data created, accessed, or modified by Mobile IDENT is maintained in EID, as mentioned above fingerprints and photographs are only stored in IDENT.

User Account Management (UAM) Module

UAM is an application that creates and maintains user accounts for the other ENFORCE applications described above. The UAM centralizes the storage and management of user data, user accounts, and user-associated role assignments for all other ENFORCE applications. UAM eliminates the need to maintain user data within each ENFORCE application.

EID Data Collection and Users

Data that is added to the EID during the course of the described activities is either manually entered by an authorized user or electronically transmitted to update an EID record via a system-to-system interface. EID information is directly collected from aliens, suspects, associates, and witnesses during the course of immigration and criminal law enforcement and investigative activities.

Users of ENFORCE applications are DHS law enforcement agents/officers (which include ICE Agents and Officers; CBP Officers and Border Patrol Agents, Office of the Inspector General Special Agents, and Task Force Officers), immigration officers (including U.S. Citizenship and Immigration Services (USCIS) Adjudication Officers and Asylum Officers), and law enforcement support personnel.

Typical Transactions

Criminal Arrest: A DHS officer/agent arrests an individual for violating a criminal statute and brings him or her to a federal facility for booking. The officer/agent creates an event using EABM to capture the date, time, location, charges, and other details of the arrest. The officer/agent captures the subject's fingerprints using an approved electronic fingerprint scanning device and the WebIDENT application. The officer/agent also enters into EABM addresses, employment records, phone numbers, and other pertinent information, such as historical criminal and immigration data, attorney information (if any), law enforcement agencies that assisted in the arrest and/or investigation, and a narrative describing the circumstances of the arrest. The subject is then physically booked into a U.S. Marshals Service or Bureau of Prisons detention facility for further criminal proceedings. The records in EID are appropriately updated to reflect further proceedings.

Administrative Immigration Arrest and Detention: An administrative immigration arrest follows the process described above for a criminal arrest except that the ICE officer/agent uses EABM to enter the appropriate administrative charges as well, which pertain solely to violations of immigration laws.[6] The

[6] If a subject is arrested under criminal and administrative charges, the officer/agent adds both administrative and criminal charges to the record in EID. The criminal processes are carried out first before the administrative immigration case will proceed.

officer/agent then prints the system-generated forms required to initiate immigration court proceedings to remove the subject from the United States. EABM does not allow a user to print these forms where the subject has been identified in the system as a U.S. citizen or national.

An ICE officer/agent then uses the 'Book-In/Out' function in EADM to initiate the subject's detention in an approved immigration detention facility. An immigration officer then monitors the subject's detention status and removal proceedings using EADM and EARM. If a subject is released from detention while still in the United States (e.g., released on bond), the immigration officer will use EADM to modify their custody status to show that they have been released on bond. If a subject fails to comply with the terms of their release (e.g., fails to report to a scheduled hearing) and an immigration judge subsequently orders them removed in absentia, the immigration officer will use EARM to modify their case status to reflect that they are now considered a fugitive.

Immigration Removal Proceedings: Following the administrative arrest of a subject and the initiation of removal proceedings in EABM, EARM automatically creates a removal case and assigns it to the appropriate DRO field office. Once a subject is booked into an immigration detention facility, an immigration officer uses EADM and EARM to manage the detention and to monitor the status and progress of the immigration proceedings against the subject in immigration court until completed. Using EARM, the DRO field office documents key actions and/or decisions for the proceedings such as the issuance of a removal order, the filing and outcome of an appeal, requests for and receipt of foreign government travel documents, and actual removal departure information. The EARM removal case is formally closed when the alien is removed from the United States (or voluntarily departs), or when the immigration court proceedings are concluded and the alien is permitted to remain legally in the United States.

EID Architecture

The EID exists in four technically discrete environments: development, operational, testing, and training. The development environment is used during the design and development of EID database modifications and ENFORCE applications. The operational environment stores information created during DHS immigration and law enforcement investigations and operations. This information constitutes the official records of these DHS activities. The testing environment is used during pre-deployment testing of EID database changes and ENFORCE applications. The training environment is used to conduct user training. Development, test, and training environments use dummy biometric, biographic, or encounter-related data rather than real data.

Associated data repositories, the EID Datamart (EID-DM), the EARM Datamart (EARM-DM), and the ICE Integrated Decision Support (IIDS) System, are subsets of the EID database repository that provide a continuously updated snapshot of selected EID data. The purpose of the EID-DM, EARM-DM, and IIDS is to support DHS requirements to query EID data for operational or executive reporting purposes. EID-DM, EARM-DM, and IIDS are queried instead of EID to protect the integrity of the live data held in the EID operational environment and to prevent the performance of EID and the ENFORCE applications from being diminished. Access to the EID-DM, EARM-DM, and IIDS is read-only, so no data values are changed by users that query them. These data repositories are typically used to generate management reports and statistics from EID data.

The EID-DM contains data on arrests (including information on individuals who are subjects of investigations), incidents, processing (for removal), a subject's personal property. EARM-DM contains information on those subjects who have removal cases pending or have been removed from the United States. EARM-DM information includes travel document information, information on immigration court proceedings, arrests, charges, bonds, dockets, detention facilities, and detention inspections. IIDS contains biographic information, information about encounters between agents/officers and subjects, and apprehension and detention information about all persons in EID. Throughout the remainder of this document, all general references to EID data are intended to include the data stored in EID-DM, EARM-DM, and IIDS unless otherwise stated.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The EID maintains information that is collected and used by the ENFORCE applications to support DHS law enforcement efforts in the areas of immigration, customs and trade enforcement, national security, and other criminal laws enforced by DHS. Information about each individual in the EID is documented based on event-driven encounters, such as booking, arrest, detention, and removal. Therefore, an individual may be connected to multiple records in the system, each pertaining to a different event or encounter.

The personally identifiable information (PII) maintained in EID consists of biographical, descriptive, biometric, and encounter-related data about subjects who are arrested, detained, and/or removed, or amenable to removal, for criminal and/or administrative violations of the Immigration and Nationality Act and other criminal laws enforced by DHS. Biographic data includes name(s), aliases, date of birth, telephone numbers, addresses, nationality, citizenship, Alien Registration Number (A-Number), Social Security Number (SSN), passport number, visa information, employment history, educational history, immigration history, and criminal history. Descriptive data includes data such as height, weight, eye color, hair color, and any other unique physical characteristics (e.g., scars, marks, tattoos). Biometric data consists of fingerprints or photographs captured via WebIDENT, although this information is sent to IDENT and not permanently stored in EID. Encounter-related data is information about DHS's interaction with an individual during an event including, but not limited to, event location, document numbers, encounter or arrest date, and description of event and any violations.

In addition to the data described above, EID also maintains the following types of information:

- Alias identities used by criminal suspects or immigration violators. Sometimes criminal suspects adopt the real identities of other persons as aliases, in which case PII pertaining to those individuals may be collected and maintained in EID. Alias information may include name, nationality, A-Number, date of birth, address, telephone number and other information relating to the alias identity.

- Information about relatives of those who are alleged immigration violators to provide information necessary to determine the subject's identity and nationality and/or to support an existing criminal investigation for immigration fraud in which the subject is involved or connected. This information typically consists of the relative's name(s), address(es), and place of birth.
- Birth, marriage, education, employment, travel, and other information derived from affidavits, certificates, manifests, and other documents presented to or collected by DHS during immigration and law enforcement proceedings/activities. This data typically pertains to subjects and relatives. EID also maintains information about the sources of this data.
- Information about attorneys or representatives who represent an alien in removal, immigration benefit, criminal prosecution, or other proceedings conducted or initiated by DHS. This may include the representative's name, agency or business name, address, telephone number and other information.
- Biographical, identifying, and detainee information on prisoners of the U.S. Marshals Service who are held in ICE detention facilities pursuant to an interagency agreement. This information is limited to the prisoner's name, date of birth, country of birth, detainee identification number, FBI identification number, state identification number, book-in/out date, and security classification.
- Records relating to persons who post or arrange bond for the release of a subject from custody or receive property of a detainee. This may include name, address, telephone number, SSN and other information.
- Data to describe an event involving alleged violations of criminal or immigration law including location, date, time, event category, types of criminal or immigration law violations alleged, types of property involved, use of violence, weapons, or assault against DHS personnel or third parties, attempted escape and other related information. Event categories describe broad categories of criminal law enforcement, such as worksite enforcement (immigration), contraband smuggling, and human trafficking.
- DHS case management information, including case category, case agent, and date initiated and completed. Descriptions of evidence collected during arrest, investigation, or other DHS enforcement operations.
- Detention, detainer, and transportation information related to the detention of aliens and their release from custody on bond, recognizance or supervision. A detention record includes detention facility, book-in/out date and time, mandatory detention and criminal flags, security classification level, aggravated felon status, and general health information that is relevant to detention or transportation requirements. A detention record may also include detention property, alerts, relatives, and juvenile related information.
- DNA collection information, limited to the date and time of a successful DNA sample collection and confirmation from the FBI that the DNA sample is valid. EID does not contain any actual DNA samples or sequences.

- Progress, status and final result of removal, prosecution, and other DHS processes and relating appeals. This may include information relating to criminal convictions, incarceration, and actual removal of aliens from the United States.
- Records relating to personnel of other agencies that arrested, or assisted or participated in the arrest or investigation of, or are maintaining custody of an alien who is the subject of an EID record. This can include name, title, agency name, address, telephone number and other information.
- EID user information consists of biographical data, including user name, title, official duty location, official program area, current duty location, current program area, SSN default role, supervisor name, detention facility, telephone number, call sign/star number, and user system functional roles.

1.2 What are the sources of the information in the system?

DHS collects some of the information in the EID directly from criminal suspects and alleged immigration violators. Other information is collected from witnesses, victims, or criminal associates, and from official records of other agencies, businesses, and other sources during the course of DHS mission operations including law enforcement and investigative activities. Specifically, EID obtains information from the following sources:

- Individuals, including suspects, victims, witnesses, or associates, who are questioned or interviewed by DHS officers/agents during the course of immigration and/or law enforcement investigation. This includes information retrieved from an individual's visa and immigration benefit applications, and from their travel, identity, or vital statistics documents (e.g., visa, passport, birth certificates).
- Confidential law enforcement sources.
- Official records of other agencies and courts. This includes case files, indexes, and records of organizations such as the DOS, Department of Justice (DOJ), FBI, Department of Defense (DOD), and other federal, state, local, tribal, international, or foreign governmental organizations that collaborate with DHS in pursuing DHS national security, immigration, trade, and other law enforcement, mission-related functions.
- Employers, schools and universities, witnesses, victims, criminal associates, businesses and other entities that are the source of records or information obtained by DHS during the course of an immigration and/or law enforcement investigation.
- Individuals who post or arrange for bond for subjects.
- An applicant, sponsor, or representative of an individual during the immigration benefit process and other DHS benefit and registration processes.
- Public and commercially available record sources. Public sources include local, state and national newspapers in electronic form, sex offense registries, and local law enforcement sites.

An officer/agent may also collect information from case files, indexes, and records within ICE or at other DHS offices and components, such as ICE, CBP, USCIS, Transportation Security Administration (TSA), or U.S. Coast Guard during the course of an investigation or enforcement activity. An officer/agent manually enters pertinent information into EID. EID data may also be gathered through interfaces to several DHS information systems listed below and then manually entered into EID. The Privacy Act System of Records Notices (SORNs) covering each system are also identified below, where applicable.

- ICE's Electronic Travel Document (eTD) System. eTD sends notification to EID when an electronic travel document is sent by eTD to participating consulates (requesting the electronic document) and is received. eTD data is transmitted to EID via a direct system to system interface.
- USCIS's Central Index System (CIS). Alien File and Central Index System SORN, DHS-USCIS-001 (Jan. 16, 2007, 72 FR 1755). CIS sends biographical and historical information about subjects. USCIS's data is transmitted to EID via a direct system to system interface.
- ICE's General Counsel Electronic Management System (GEMS). GEMS SORN, DHS/ICE/OPLA-001 (March 31, 2006, 71 FR 16326). GEMS provides subjects' alien file (A-File) number to EID through a direct system to system interface.
- ICE's Student and Exchange Visitor Information System (SEVIS). SEVIS SORN, DHS/ICE-001 (March 22, 2005, 70 FR 14477). SEVIS provides biographical, visa status violations, and school status information on non-immigrant students and exchange visitors. SEVIS data is manually input into EID by ICE personnel who access SEVIS via separate user accounts.
- USCIS's Refugee, Asylum, and Parole System (RAPS). RAPS provides EID with asylum information and referral information pertaining to the Nicaraguan Adjustment and Central American Relief Act of 1997. RAPS data is input into EID via a system to system connection, and manually by ICE personnel who access RAPS via separate user accounts.
- DOJ's Executive Office for Immigration Review (EOIR) Records and Management Information System (RMIS). Justice/EOIR-001 (July 5, 2001, 66 FR 35458). RMIS, an immigration case tracking and management system, provides EID a verification of immigration status, specifically providing immigration court hearing information on subjects, such as court hearing schedules and decisions, case preparation, subject's length of stay in detention, and the issuance of removal documents. EOIR data is transmitted to EID via a direct system to system interface.
- FBI's Integrated Automated Fingerprint Identification System (IAFIS). Justice/FBI-009 (September 28, 1999, 64 FR 52343). IAFIS provides EID with criminal history and associated FBI numbers of subjects. IAFIS data is input into EID through manual entry by ENFORCE users and via a system to system interface.
- State Department's Consular Affairs Consolidated Database (CCD). Visa Records SORN, STATE-39. EID users query CCD and manually input into EID the information from an alien

visa application, including U.S. and foreign addresses, biographical information, and passport information.

- Alien data is also received from the IDENT application (DHS/USVISIT-0012, Jun. 5, 2007, 72 FR 31080), which stores fingerprint and/or photographic and limited biographic data collected for national security, law enforcement, immigration, intelligence, and other mission-related functions. IDENT provides EID with certain information on subjects such as port of entry information, biographical and identifying information, including name, date of birth, visa and passport information. All data except the Fingerprint Identification Number is input manually into EID by ICE personnel who have IDENT user accounts. The Fingerprint Identification Number is electronically transmitted from IDENT to EID via a system to system interface.

1.3 Why is the information being collected, used, disseminated, or maintained?

DHS officers/agents capture this information for the purpose of conducting investigations, operations and other enforcement and case management activities related to the enforcement of U.S. immigration laws and federal criminal laws enforced by DHS. The information is collected and used to support the following DHS activities:

- Identifying, apprehending, and removing individuals who are in the United States illegally.
- Investigating, identifying and arresting individuals (both U.S. citizens and non-U.S. citizens) who commit violations of federal criminal laws for which DHS/ICE has enforcement authority.
- Conducting background checks related to requests for DHS immigration benefits (e.g., employment authorization and petitions).
- Tracking the process and results of criminal or civil proceedings against individuals or organizations who commit illegal acts.

1.4 How is the information collected?

Data is added to EID in one of two ways. First, EID users may manually input data into EID obtained from other systems or sources (such as the subject, identity documents, etc.). Second, EID may receive the data electronically from another system, typically on a real-time basis, through an extract or system-to-system connection. EID information is directly collected from subjects, witnesses, victims, criminal associates and other individuals and entities (described in Question 1.2 above) during the course of law enforcement and investigative activities, or during the immigration benefits process (e.g., EID may contain data retrieved from an individual's application for immigration benefits). EID information may be electronically or manually obtained depending on the source. Information may also be obtained by approved undercover operations, some of which include the use of electronic surveillance technology.

Biometric information, such as fingerprints and photographs, is collected from the individual electronically using biometric collection devices.

EID does not receive a regular load of data from other systems but makes ad hoc queries when new records are created or updated. Users of ENFORCE applications only have the ability to initiate queries and receive replies on a case by case basis from outside sources, such as the FBI IAFIS and the DOS Consolidated Consular Database.

1.5 How will the information be checked for accuracy?

Much of the EID information is collected directly from the individual or the individual's identity and travel documents during law enforcement encounters, the immigration benefits and enforcement process, or other DHS activities or proceedings, thereby increasing the likelihood that the information in EID is accurate. EID information is also subjected to data quality review processes established to detect employee errors and make appropriate corrections. For example, EID information is reviewed by an agent/officer's first line supervisor before a criminal or administrative process is allowed to proceed. Each of the ENFORCE applications also have field-level checks on data to ensure a minimum level of quality and completeness.

Additionally, EID users undergo mandatory user training for the system during training for new officers and agents. This training also covers topics such as immigration and customs laws, the administrative removal process, and investigative methods. Other more general training courses and resources for law enforcement personnel also emphasize the importance of verifying information prior to using it for enforcement activities. Specifically, ICE law enforcement personnel are required to adhere to the ICE Case Management Handbook and complete ICE Integrity Training and privacy/security training annually, all of which stress the need to verify information and the techniques for doing so. When new or updated policies and procedures are implemented, users are notified via electronic announcements.

In some instances inaccurate information may be captured and stored in EID because of a misunderstanding of the information provided by individuals or because of untruthful statements made by subjects during interviews for various reasons, such as a desire to conceal criminal conduct, associates, or their actual identities. That said, some erroneous statements may not be detectable or verifiable, and as a result become a part of official law enforcement records and relied upon in subsequent DHS proceedings. Similarly, when information about an individual is received from other sources, the record that is created memorializes the information provided by the source and may not be independently verifiable (e.g., claims by witnesses). Also, for covert and ongoing law enforcement investigations, directly verifying the accuracy of information in EID with the suspect is not possible without seriously undermining the investigation by potentially compromising the identities of sources and alerting the suspect to the existing investigation.

When DHS officers/agents discover inaccurate data 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, the user need only correct the data in a single ENFORCE application to ensure the data is corrected throughout EID. The use of biometrics also enhances accuracy by revealing the existence of individuals whose identity records contain conflicting information. The use of fingerprints and photos

provides a method for quickly determining if conflicting identity data exists about the same individual, and allowing any discrepancies to be resolved. The collection of name and date of birth alone would not serve as well in accurately identifying individuals, as repeat offenders have been known to provide a variety of names and dates of birth during law enforcement encounters to avoid identification and association with past crimes or violations.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

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. § 1324(b)(3); 8 U.S.C. § 1357(a); 8 U.S.C. § 1360(b); 19 U.S.C. § 1; and 19 U.S.C. § 1509. Additional authority is provided in 6 U.S.C. §§ 202; 8 U.S.C. 1158, 1201, 1365a, 1365b, 1379, and 1732; and 19 U.S.C. §§ 2071, 1581-1583, and 1461; and the Immigration Reform and Immigrant Responsibility Act of 1996.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: There is a privacy risk that PII in the system may be accessed or altered by unauthorized individuals for criminal or other unauthorized purposes.

Mitigation: The privacy risk is minimized by the EID architecture, which is maintains PII in a single data repository and system rather than data in separate applications and systems in different locations, but linked together to provide the required functionality. This structure reduces the risk to the data by minimizing its proliferation in multiple locations and systems, each of which would need to employ physical or technological security measures to prevent a breach. Authentication and role-based user access requirements ensure that users only can access or change EID information that is appropriate for their official duties. DHS supervisors determine the user roles and access requirements of their subordinates, and a user account may only be established after written supervisory approval is provided. In addition, background checks are conducted on users to ensure they are suitable for authorized access to EID. The effectiveness of authentication and security protections are verified through audits of system operation and usage.

Privacy Risk: There is a privacy risk that information will not be accurate and timely.

Mitigation: The EID architecture is designed to minimize the risk that EID will contain stale and inaccurate data by maintaining all data in a single repository that is acted upon by the various applications. Because of this system design, updates to data made by a user in one ENFORCE application are immediately available to users in all other ENFORCE applications (to the extent such users have privileges to use those applications and view the data in question).

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

ICE uses the information in EID to support ICE's activities to arrest, detain, and remove aliens from the United States in accordance with U.S. immigration law, including the identification, arrest and removal of fugitive aliens and the provision of health care to aliens in detention. The EABM component of EID is also used to document all criminal arrests by participating DHS law enforcement components, regardless of the arrested person's nationality or immigration status. EID's report generating capability also allows ICE to use the system to provide statistical reports on these activities to ICE and DHS management.

DHS-ICE officers/agents use the information in EID to record the arrests of individuals for criminal activity and for administrative and criminal violations of the U.S. immigration laws. These officers/agents also use EID to obtain information on previously arrested subjects in support of current investigations or prosecutions. These officers/agents also use EID information to support the management of ICE detention and removal activities, including the management of detention facility assignments, bed space, transfer of detainees among detention facilities, and coordination of travel to remove aliens from the United States.

Subjects' SSNs are collected in order to properly identify individuals and to provide information to the Social Security Administration (SSA) if and when subjects are removed from the United States. Subject fingerprints and the Fingerprint Identification Number are used to confirm identity and obtain criminal history information about the subject, including previous encounters, previous immigration encounters, and wants and warrants. Data from commercial sources are used to assist ICE officers/agents in the verification of subjects' former and current places of residence, former and current cohabitants, as well as identifying personal properties owned by these subjects. Data obtained from public sites aid in confirming the identity and contact information of subjects, criminal activity, affiliations, current and previous employment, custody-related information, and past and current humanitarian state of an alien's country of citizenship.

Employees in other DHS components – CBP, USCIS, U.S. Coast Guard, and US-VISIT – also have access to EID information. In support of its responsibility to decide whether to admit an individual the United States, CBP uses EID information to conduct immigration status checks, search for and review criminal history of subjects, as well as obtain subject lookout information on individuals encountered by CBP at the border and during enforcement activities by CBP Border Patrol Agents and Officers. USCIS uses EID to research an individual's immigration history to determine if an individual is eligible for an immigration benefit for which they have applied. U.S. Coast Guard uses EID information to conduct immigration status checks and checks on criminal history, previous encounters, and wants and warrants (obtained through the IDENT and IAFIS fingerprint check) on individuals who are persons of interest in

U.S. Coast Guard maritime enforcement activities. In addition, EID information is used to conduct statistical reporting on mission-related activity, led by DHS management.

As described in Section 4.0, other federal systems, inside and outside of ICE, use EID-created data extracts to support immigration, national security, and law enforcement efforts by ICE, DHS, and other federal agencies. As described in Section 5.0, on a case-by-case basis, ICE's state, local and foreign law enforcement partners also use EID data to aid in criminal law enforcement and homeland security activities.

2.2 What types of tools are used to analyze the data and what type of data may be produced?

EID can run simple reports based on the total number of recorded immigration encounters, locations, and judgments for internal reporting and analysis, performed by ICE management. Specifically, these reports aid in setting and evaluating law enforcement strategies, target goals, training and development activities, hiring and staffing, and system enhancement efforts.

2.3 If the system uses commercial or publicly available data, please explain why and how it is used.

As described in Question 1.2 above, ICE subscribes to commercial public record aggregators. ICE is also able to leverage public law enforcement sites, local, national, and international news sites, telephone directories, and similar sites, which are all publicly available via the Internet. Data collections from commercial sources are used to assist ICE officers/agents in the verification of subjects' former and current places of residence, former and current co-habitants, as well as identifying personal properties owned by these subjects. Data obtained from public sites aid in confirming the identity and contact information of subjects, criminal activity, affiliations, current and previous employment, custody-related information, and past and current humanitarian state of an alien's country of citizenship. Information obtained is then manually entered into EID to assist with ongoing investigations or other DHS mission functions. This information is verified through approved and standardized methods, including but not limited to interviews, subpoenas, and surveillance.

EID does not electronically interface with commercial or public sources or systems directly. ICE officers/agents obtain data from these sources on an ad hoc basis and manually enter relevant information into EID.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Various controls exist to ensure that information is handled in accordance with the uses described in this PIA. Security policies and procedures are in place to ensure that only authorized users have access to the system, and enhanced user roles are being developed to ensure that individual users have access levels that are appropriate only to their role. Additionally, system users are audited to track who accesses

the system and what changes are made to system data so that inappropriate uses can be detected and redressed.

Information obtained from public and commercial data sources is verified during the law enforcement process through various means, including interviews with the data subject, corroboration from independent sources, and other government information systems that have high-quality data or are the actual source of the data obtained from the commercial/public source. Corroboration and verification of information obtained from commercial or public sources is required before actions against the individual may be taken in a criminal or administrative matter.

All system users also undergo mandatory training on appropriate usage of the system and the data. In addition, all DHS personnel undergo security and privacy training, which raises awareness about the importance of the need to secure and appropriately use sensitive personal data. Limited direct access to the system, audit trails, and training regarding appropriate usage of the information ensure that data is used in accordance with the allowed uses and to minimize the risk that personal information will be accessed by unauthorized individuals.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

ICE retains primary EID records which consist of all booking, detention and removal records in EID. ICE also retains U.S. Marshals Service prisoner detention records; fingerprints and photographs in the Mobile IDENT laptop cache; EID-DM, EARM-DM, and IIDS records; user account management records; statistical records; audit files; and backup files.

3.2 How long is information retained?

ICE anticipates maintaining primary EID records for 100 years. These records are proposed to be retained 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. Records concerning U.S. Marshals Service prisoners will be retained for ten (10) years. Fingerprints and photographs collected using Mobile IDENT are retained for up to seven (7) days in the cache of the encrypted U.S. Government laptop then maintained in IDENT for 75 years. EID-DM, EARM-DM, and IIDS records will be retained for 75 years to allow for reporting and long-term trend analysis.

User account management records will be kept for ten (10) years following an individual's separation from Federal Government service. If an investigation revealed that a particular user accessed a record and changed it, and a record is not kept on who the user is, the ability to identify and investigate employee misconduct would not be possible. In addition, ICE is proposing to maintain statistical records for ten (10) years, audit files for 15 years, and backup files for up to one (1) month.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. A retention schedule was approved by NARA for the enforcement information described above when these records were maintained by the former U.S. Immigration and Naturalization Service. ICE is proposing to modify this retention schedule in accordance with the proposed retention periods stated in Question 3.2 above..

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: There is a privacy risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: The information in EID is retained for limited periods appropriate to the purpose of the system. For example, the system retains information about aliens who are arrested and removed for violations of U.S. immigration laws for at least the lifetime of those aliens. Accordingly, the information is retained for a time that is limited and appropriate.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

EID data is shared outside of ICE with other DHS components and offices. Specifically, EID data is accessible by various personnel at CBP, USCIS, US-VISIT, and U.S. Coast Guard who are granted EID user accounts to assist them in performing their missions. Moreover, these agencies only have access to the EID applications and data that are relevant to their respective missions and authorities. Specifically, CBP uses EID information to conduct checks on individuals encountered by CBP at the border and during enforcement activities by CBP Border Patrol Agents and Officers. EID information supports CBP's use of US-VISIT's information in admission decisions.

USCIS uses EID to research an individual's immigration history prior to issuing immigration benefits to ensure the individual is eligible for the benefit sought. U.S. Coast Guard uses EID information to conduct immigration status checks and checks on criminal history, previous encounters, and wants and warrants on individuals who are persons of interest in Coast Guard maritime enforcement activities.

EID event and biographic information is exported to other ICE systems, ICEPIC and the Law Enforcement Intelligence Fusion System (IFS), to support the law enforcement purposes of those systems

and to allow DHS users of those systems, including DHS Intelligence and Analysis personnel, to analyze EID information in conjunction with other information to produce reports relating to law enforcement and terrorism threats.[7]

ICE also exports EID information electronically via file transfer protocol (FTP) or email to the following DHS systems to support their law enforcement and/or immigration related purposes:

- CBP's TECS – EID exports information about fugitive aliens, such as those aliens who have been classified as absconding from a judges removal, and aliens who have been removed from the United States to support CBP's screening at ports of entry and other law enforcement activities.
- CBP Materialized Views – EID shares biographical, apprehension, and assault data as needed with this CBP reporting tool application to allow CBP to generate statistical reports about CBP law enforcement activities recorded in EID.
- CBP Seized Asset and Case Tracking System (SEACATS) – EID provides SEACATS with seized assets information, biographical and identifying data, and subject arrest information necessary to conduct asset forfeiture proceedings.
- CBP Secure Border Initiative (SBI) Federated Query – This system queries information in EID-DM about individuals arrested, detained, or removed from the United States under immigration laws. CBP has access to this information to support its efforts to identify both criminal and illegal aliens at border crossings.
- USCIS Central Index System – EID provides biographic and removal information to this system in support of USCIS's alien registration and immigration services processes. This information helps USCIS properly adjudicate requests for immigration benefits based on the requirements of the Immigration and Nationality Act and other federal regulations to prevent individuals from unlawfully obtaining immigration benefits.
- US-VISIT's IDENT application – EID shares event and biographic information for subjects arrested, detained, or removed from the United States under immigration laws to support the US-VISIT program, which is intended to establish and verify the identity of persons during entry and exit processing at the border and to assist CBP in determining the admissibility of non-U.S. persons.

4.2 How is the information transmitted or disclosed?

In most cases, a data file is transmitted between EID and other systems on the DHS core network, an unclassified, secured wide area network via FTP or email. Other types of transmission or disclosure, such as provision of a compact disc containing a data file, may be required in some circumstances. For example, some information is provided by exchanging printed copies of EID records.

---

[7] *See* ICEPIC and Intelligence Fusion System Privacy Impact Assessments at www.dhs.gov/privacy.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: There is a risk that the scope of internal sharing exceeds the purposes for which the information was originally collected.

Mitigation: This risk is mitigated by the fact that in most cases DHS internal data sharing is required by law or DHS policy to allow other DHS components to carry out their missions or to enforce statutory requirements for border and national security and law enforcement.

Privacy Risk: There is also a privacy risk that individuals without a need to know will access the data, or will use it inappropriately.

Mitigation: This risk is mitigated by the controls described in Sections 2 and 8 by which the data are kept secure, accurate, and appropriately controlled. EID employs access controls and audit trails and all DHS personnel are required to complete annual security and privacy training, which mitigates the risk that information will be used inappropriately by authorized users. This also mitigates the risk that the information will be provided to individuals without a need to know.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS, which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Through ICEPIC, EID event and biographic information is made available to other federal, state, local and tribal law enforcement agencies through the DHS Law Enforcement Information Sharing Service. Using this Service, EID data is shared with sworn law enforcement officials subsequent to an approved law enforcement sharing agreement between DHS and the law enforcement agency or the law enforcement sharing network of which the law enforcement agency is a member. The PII extracted from EID is shared via a secured Law Enforcement Information Sharing Service connection.

On an ad hoc basis, DHS shares EID information with federal, state, local, tribal, foreign, or international government agencies and task forces that demonstrate a need to know in the performance of their missions consistent with DHS national security, law enforcement, immigration, trade, intelligence, or other mission-related functions. EID information is also shared on an ad hoc basis with intelligence agencies or fusion centers that are lawfully engaged in collecting and producing law enforcement intelligence. EID information is shared with other federal agencies in the course of collaborating, assisting, and supporting national intelligence and security investigations.

Under the provisions of Section 287(g) of the Immigration and Nationality Act, authorized law enforcement officers working for U.S. state and local law enforcement agencies may be formally

delegated authority to act as DHS law enforcement officials for the purpose of enforcing U.S. immigration laws.[8] These officers are provided user accounts to the EABM and other ENFORCE applications in order to conduct checks by searching removal information in EID, create booking records when they arrest, identify, process, and when appropriate, detain immigration offenders they encounter during regular, daily law enforcement activity.

DHS also shares EID data with other government agencies when disclosure is necessary to elicit information required to carry out DHS functions, or respond to lookouts or notifications. Where an EID record indicates, either on its face or in conjunction with other information, a violation or potential violation of criminal or civil law, the relevant records may be referred to the appropriate federal, state, territorial, tribal, local, international, or foreign agency law enforcement authority or other appropriate agency charged with investigating or prosecuting such a violation or enforcing or implementing such law.

The EID information is also shared with the following external organizations:

- SSA
    - For removed aliens only, the names, aliases, SSNs, dates of birth, gender, country of birth, country to which removed, date of removal, and the A-Number are disclosed in the form of an electronic extract to SSA. The purpose of the disclosure is to assist SSA in determining the identity of any Social Security number holder who has been removed and may be subject to nonpayment of Social Security retirement and/or disability benefits, or suspension of their SSI payments. This extract is provided on a recurring basis and transmitted to SSA via a secure file transfer protocol server. At SSA, the data is compared against the following SSA systems: Master Files of Social Security Number Holders (NUMIDENT) – SSA/OEEAS 60-0058 January 11, 2006, 71 FR 1815; Master Beneficiary Record (MBR) – SSA/OEEAS 60-0090 January 11, 2006, 71 FR 1826; and Security Income Record and Special Veterans Benefits (SSR/SVB) – SSA/ODSSIS 60-0103 January 11, 2006, 71 FR 1830. SSA does not retain any information unless a match is found and verified.
- FBI
    - Biographical and removal information on aliens allegedly charged criminally or administratively is provided to the FBI in accordance with its authority to investigate criminal or administrative violations of the Immigration and Nationality Act. This is an automated electronic extract that is provided on a recurring basis and transmitted via a secure file transfer protocol server pursuant to an Interconnection Security Agreement (ISA). The data is loaded into the FBI's Integrated Automated Fingerprint Identification System (Justice/FBI-009, September 28, 1999, 64 FR 52343), through the U.S. Marshals Service Joint Automated Booking System (JABS) (Justice USMS-005, January 25, 2007, 72 FR 3410).

[8] *See* 287(g) Database PIA at www.dhs.gov/privacy.

- Biographical and identifying information on subjects, including but not limited to A-Number, FBI number, fingerprint identification number, date of birth, race, citizenship, and sex to support the DNA sample collection process. (DNA samples and sequences are not stored in EID.)
- To the FBI's National Information Check System (NICS) – (Justice/FBI-018, November 25, 2008, 63 FR 65223). As required by 18 U.S.C. § 922(g) or (n), EID transfers biographical data to NICS on persons barred from purchasing firearms under the Brady Act. EID provides identifying information along with associated criminal activity on subjects. This information aids in determining whether to grant or deny a firearm license to an individual.
- To the FBI's Foreign Terrorist Tracking Task Force (FTTTF) – EID shares biographical, identifying, visa origin of citizenship, and removal information to support FTTTF terrorist prevention and investigation efforts.

- Department of State
  - Biographical and removal information and notification relating to the cancellation of visas to support DOS visa issuance. This is an automated electronic extract that is provided on a recurring basis and transmitted via a secure file transfer protocol server. The data is loaded into the DOS's Consular Lookout and Support System (CLASS), Visa Records SORN, STATE-39 and Passport Records SORN, STATE-26.
- Department of Justice, Executive Office of Immigration and Review (EOIR)
  - Information on active detentions is provided to support proper coordinating and scheduling of immigration hearings and removal proceedings. This is an automated electronic extract that is provided on a recurring basis and transmitted via a secure file transfer protocol server. The data is loaded into EOIR's Records and Management Information System.
- Foreign Embassies and Consulates
  - Biographical information relating to aliens apprehended by DHS who are nationals of the country the embassy or consulate represents to comply with international treaties and agreements. This information is provided on an ad hoc basis in the form of electronic extracted information.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing described above is compatible with the original purpose for collection, namely to conduct criminal law enforcement investigations and other enforcement activities, including the enforcement of U.S. immigration laws. All external sharing falls within the scope of published routine uses in the DHS/ICE-011 Immigration and Enforcement Operational Records (ENFORCE) System of Records. The ENFORCE SORN is being republished and updated concurrently with this PIA.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is generally transmitted manually or disclosed orally to external organizations on an ad hoc basis pursuant to a routine use defined in the ENFORCE SORN or in response to a request under section (b)(7) of the Privacy Act. External organizations do not have direct access to EID, meaning that external organizations do not have access through individual user accounts. External organizations secure EID information in accordance to the terms of information sharing agreements which include provisions for appropriate and adequate safeguarding of sensitive information.

Information transmitted electronically to certain external organizations is done through external interface connections in encrypted form, bounded by Interconnection Security Agreements and Memoranda of Understanding. Information shared via external interfaces is done routinely and shared in bulk. External partners that do not have the capability to exchange data through an automated process receive data via encrypted e-mail or encrypted DVD/CD via carrier service.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

There is a potential risk of EID information being leaked, misused, or lost by the agencies with which DHS shares EID information. The EID information that DHS shares with an external entity is tailored to contain only information that is required by the requesting or receiving agency. In addition, access to EID data by interface from other agencies' databases is controlled by a user ID and password and requires a service level agreement between DHS and the other agency that defines requirements for network and interface security. The response provided in Question 1.7 is relevant to the risks relating to sharing EID information with external organizations.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

As noted above, some of the information in the EID is collected directly from a suspect after a criminal or administrative arrest. In such cases, the individual is advised in writing and orally of their right to refuse to provide information pursuant to the Fifth Amendment. With respect to information obtained from suspects or other individuals through government forms, such as immigration benefit applications, Privacy Act statements on those forms provide notice to the individual that their information may be shared with law enforcement entities.

During the course of a law enforcement investigation, it is not feasible to provide individuals who are interviewed as suspects, witnesses, or victims with any form of written notice regarding the collection of information, nor is such written notice required by the Privacy Act or other federal laws or policies. With the exception of authorized undercover operations, however, these individuals are aware they are being interviewed by a law enforcement officer and that their information is being collected for use in an investigation.

More generally, this PIA and the updated ENFORCE SORN (published concurrently with this PIA) serve as public notice of the EID and its related ENFORCE applications.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

In most cases, because of the DHS law enforcement or immigration purposes for which the information is collected, opportunities to decline may be limited or nonexistent. Users may enter data during the course of a law enforcement activity or in support of other DHS proceedings, and it is the nature of the proceeding and the individual rights afforded to the subject by law that will determine the ability of a person to exercise the right to decline to provide information. In the case of administrative or criminal arrest, the individual is advised of his or her right to refuse to provide information pursuant to the Fifth Amendment. Other information is collected in application forms submitted to DHS to receive immigration or other benefits. In such cases, a Privacy Act notice is printed on the application form advising the applicant of any right they may have to decline to provide information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

In most cases, because of the DHS national security, law enforcement, immigration, or intelligence purposes for which the information is collected, no such consent exists. In the case of administrative or criminal arrest, when the individual is advised of his or her right to refuse to provide information pursuant to the Fifth Amendment, the notice of rights informs the individual that the information they provide will be used in proceedings against them. By providing information after receiving such a warning, the individual consents to any lawful use of the information. The only means by which the individual can withhold consent to any particular use of information is to refuse to provide the information.

Information is collected in application forms submitted to DHS to receive immigration or other benefits. In such cases, a Privacy Act notice printed on the application form advises the applicant of the intended use of the information. Submitting the application constitutes an individual's exercise of the right to consent to use of the information.

As discussed in Question 1.5 above, it may be infeasible, or operationally inadvisable, to obtain consent of the individual before using information about him or her that is provided by another source.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Because the data stored in EID is used in support of systems where law enforcement or intelligence contexts apply, notice or the opportunity to consent to use would compromise the ability of the agencies to perform their missions and could put DHS personnel at risk. Thus, notice of collection and consent to specific uses are limited or not available in most cases for data stored in the EID; however, the methods of providing direct notice as appropriate to an individual are described in Section 6.1 above. There is a potential risk that an individual may not understand the notice. When necessary, the notice to an arrested person is provided in their native language through an interpreter or through written translation. There is a potential risk that false or misleading information about an individual may be provided by a source with malicious intent. This risk is mitigated by user training and standard operating procedures that emphasize the importance of verifying information prior to recording and using it.

A risk exists that the public is not aware of EID and the associated ENFORCE applications. This risk is mitigated by providing notice of the EID through this PIA and the ENFORCE SORN.

There is a countervailing risk that arises when an individual is notified that information is being collected about them by DHS for a law enforcement or intelligence purpose. The notification may cause the individual to flee or destroy or conceal evidence required by DHS, compromise the ability of DHS agencies to perform their missions, and could put DHS personnel and resources at risk of injury, death, loss, or destruction. In such cases, DHS will intentionally withhold notification to the individual until he or she is arrested or indicted.

Section 7.0 Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

DHS has exempted the ENFORCE system of records from access requirements pursuant to 5 U.S.C. § 552a(j) and (k). This is because access to the EID records could inform a subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of

DHS or another agency. This could enable the individual who is the subject of a record to impede the investigation, to tamper with witnesses, destroy or conceal evidence, and flee to avoid detection or apprehension. In addition, permitting access to such information could disclose protected critical infrastructure information that could be detrimental to homeland security.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528. Requests for access will be reviewed on a case-by-case basis to ensure that the records meet the requirements set out by the Privacy Act as well as preserve the evidentiary value and integrity of DHS records.

Access to certain information, such as the particulars concerning an arrest or rights advisements that were provided contemporaneous to an arrest, will be provided to legal counsel and/or the individual where a lawful requirement to provide such information exists. In addition, most or all of the information collected by DHS may be disclosed to an individual pursuant to federal rules of civil or criminal procedure upon appropriate discovery order of a court.

7.2 What are the procedures for correcting inaccurate or erroneous information?

DHS is exempting the ENFORCE system of records from record correction requirements pursuant to 5 U.S.C. § 552a(j) and (k). As discussed in Questions 1.5 and 7.1, DHS may determine that the evidentiary value of false information intentionally provided to DHS prevents the correction of a record, but may create a new record to reflect corrected information.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528. As noted above, DHS has exempted the system from record correction requirements generally; however, requests for correction of records will be reviewed on a case-by-case basis to ensure that the records meet the requirements set out by the Privacy Act and preserve the evidentiary value and integrity of DHS records.

In addition, an individual may challenge user mistakes and the errors or untruthfulness of a witness in the evidence and testimony presented in relevant criminal or civil proceedings. The individual may also petition a court to direct DHS to expunge or correct an error in an EID record.

7.3 How are individuals notified of the procedures for correcting their information?

This PIA and the ENFORCE SORN (to be published concurrently with this PIA) serve as public notice of the access and record correction procedures. The notice informing a requester that he or she will be permitted access to review EID records will include notice of the procedures for requesting a correction of EID information.

7.4 If no formal redress is provided, what alternatives are available to the individual?

If an individual is not satisfied with the response, he or she can appeal his or her case to the appropriate authority provided for in the Privacy Act. There may also be specific legal remedies available to the individual in the context of any criminal or immigration proceedings in which the individual is involved.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

DHS personnel are the only persons with the ability to add, update, or delete EID data. They work with the individual under removal proceedings to insure that the data is correct and a case is adjudicated correctly.

There is a potential risk that a request for access or to correct information about an individual may be an attempt to determine whether DHS is aware of a threat to homeland security or an intended or ongoing crime or to eliminate information in DHS systems that relates to an as-yet-undiscovered threat or crime. This risk is mitigated by user training and standard operating procedures that emphasize the importance of fully reviewing all DHS information prior to granting access or agreeing to correct a record.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

User requests for access to EID must be approved in writing by a user's supervisor to ensure that access is appropriate and related to the individual's duties. A user request form (Form G-872) is completed and signed by the supervisor. The roles and privileges assigned to a particular user dependent on that user's job responsibilities. EID and the ENFORCE applications further restrict users' access to specific functions based on the role assigned them. ICE is currently revising UAM to define a number of user roles that are assigned to grant specific privileges to users based on their functions. The assigned user role determines what ENFORCE application(s) a user may access and whether a user has read-only access, report-only access, write privileges, or administrator privileges. Examples of the user roles include

officer/agent users, booking-only users, supervisors, read-only users, data entry users, reports-only users, help desk users, and super users. The privilege to assign roles is limited to supervisors and network administrators only.

8.2 Will Department contractors have access to the system?

Yes, contractors have access to the system for purposes of IT development, operations, maintenance, and support. The contractor supervisor and relevant DHS program manager use Form G-872c to authorize initial access, similar to what they do for all other EID and ENFORCE users. All contractors undergo an extensive background check prior to being granted any user privileges.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

ICE provides all EID users with system-specific training during initial entry training on all ENFORCE modules, described in the Overview section. Additionally, all ICE employees and contractors are required to complete annual privacy and security training on securely handling sensitive information at the DHS and ICE level. Also, users are given mandatory computer security awareness training and must initially and every 90 days thereafter digitally sign a "Rules of Behavior" agreement, which includes provisions to protect sensitive information from disclosure to unauthorized individuals or groups.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. There are several C&As that cover the EID applications and systems described in this PIA. WebIDENT and EABM are covered within the same accreditation boundary, and were accredited on May 21, 2007. The EADM application interface with the EID-DM is a part of the EID-DM accreditation boundary, and was accredited on November 20, 2007. The EARM application and its interface with EID are covered independently and were accredited on July 17, 2008. UAM is covered under yet another accreditation boundary, which was accredited on August 24, 2007.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The EID and ENFORCE applications secure data by complying with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. ENFORCE is periodically evaluated to ensure that it complies with these security requirements. Technical safeguards include measures such as automatic session lockout after a period of inactivity, automatic account lockout after three failed logon attempts, strong password requirements, and

deployment of firewalls that protect network connections and prevent unauthorized access. Physical access is limited to authorized personnel and network security monitoring.

In addition, the ENFORCE applications have a robust set of access controls including role-based access and interfaces, which limit individuals' access to only the data to which they should have access. Access controls include the ability of certain users to apply ad-hoc security restrictions to particular records. Misuse of data in the EID is prevented or mitigated by maintaining audit trails—including, at a minimum, records created, modified and deleted—and by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of the system. System administrators routinely review audit logs. All DHS agent/officer users' supervisors can randomly review audit trails to assess compliance with security and privacy policies, although there is no specific requirement to do so. Audit trails are reviewed by supervisors if misuse is alleged or suspected. A periodic audit and assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risks that personal information will be accessed and used inappropriately are mitigated by the use of audit mechanisms that log and monitor user activity. Security training that discusses how to protect sensitive information also mitigates these risks. The assignment of roles to users to establish their access requirements, based on their functions and information needs, along with regular review of those roles, mitigates the risk that users will be able to access information that they are not authorized to access. Users have limited access that is established based on their roles. Users with direct access to EID information and ENFORCE applications are trained in the handling of personal information. DHS networks, EID database servers, and ENFORCE application servers are protected by firewalls, access controls, intrusion detection, and antivirus protection technologies to prevent unauthorized access to the EID and alternation or destruction of EID data. DHS has procedures in place to ensure that all information system resources including the EID and ENFORCE applications go through a system security certification and accreditation process that reviews those security mechanisms and procedures that are in place and ensures they are operating in accordance with established policy.

Section 9.0 Technology

9.1 What type of project is the program or system?

The EID and ENFORCE applications are an operational IT project. EID and ENFORCE applications were originally developed for the former Immigration and Naturalization Service.

9.2 What stage of development is the system in and what project development life cycle was used?

The EID and ENFORCE applications are in the operations and maintenance phase of the system development life cycle.

9.3 Does the project employ technology which may raise privacy concerns? If so, please discuss its implementation.

No.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security