# Privacy Impact Assessment Update
# for the

# Enforcement Integrated Database (EID) – EAGLE, EDDIE, and DAVID

## DHS/ICE/PIA-015(j)

## May 14, 2019

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

**Alysa D. Erichs**
**Acting Executive Associate Director**
**Homeland Security Investigations**
**U.S. Immigration & Customs Enforcement**
**(202) 732-5100**

**Reviewing Official**
**Jonathan R. Cantor**
**Acting 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 used by several DHS law enforcement and homeland security applications. EID stores 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), U.S. Citizenship and Immigration Services (USCIS), and U.S. Customs and Border Protection (CBP), all components within DHS. The Privacy Impact Assessment (PIA) for EID was first published in January 2010.[1] Since its publication, the PIA has been updated several times to reflect the expansion of information stored in EID, the types of information shared with external parties, and an enhanced electronic sharing capability. This PIA update is being conducted to address certain applications that use EID data for the identification of individuals encountered and/or arrested by ICE. This PIA update will:

- Discuss how the DHS Office of Biometric Identity Management (OBIM) uses the EID Arrest Graphical User Interface (GUI) for Law Enforcement (EAGLE);
- Introduce the EAGLE DirecteD Identification Environment (EDDIE); and
- Introduce the Digital Application for Victim Witness Identification (DAVID).

ICE is publishing this PIA because EAGLE, EDDIE, and DAVID all process personally identifiable information (PII) about ICE investigation subjects and/or individuals subject to removal from the United States.

## Overview

EID is a common database repository owned and operated by ICE that supports law enforcement activities of certain DHS components. EID is the repository for all data created, updated, and accessed by a number of software applications. The applications that capture and use data maintained in EID capture information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and law enforcement investigations and operations conducted by ICE, USCIS, and CBP. Applications using EID data also allow users to generate immigration-related forms to send to courts and other agencies to support the advancement and adjudication of DHS and Department of Justice immigration cases. This PIA update will discuss one new way that DHS is using EAGLE and will assess the privacy risks of EDDIE and DAVID.

[1] See DHS/ICE/PIA-015 Enforcement Integrated Database (EID), January 14, 2010, *available at* www.dhs.gov/privacy.

*EAGLE*

EAGLE, the EID Arrest Graphical User Interface (GUI) for Law Enforcement, is a booking application used by ICE law enforcement agents and officers to process the biometric and biographic information of individuals arrested and detained by ICE for alleged criminal violations of law and administrative violations of the Immigration and Nationality Act (INA).[2] Since the publication of the EAGLE PIA in 2012, DHS has expanded the ways in which Department personnel use EAGLE. Specifically, DHS OBIM uses EAGLE to read fingerprint cards and retrieve an individual's Fingerprint Identification Number (FIN) to respond to Freedom of Information Act (FOIA) requests.

*Using EAGLE to Retrieve FIN for FOIA Purposes*

DHS OBIM periodically receives fingerprint cards as part of FOIA requests. To properly respond to such requests, OBIM must match the fingerprints on the cards with the individuals' FINs. However, OBIM does not have an independent query capability for its Automated Biometric Identification System (IDENT) using fingerprint cards. To alleviate this shortcoming, ICE allows OBIM to run a "search only" query in EAGLE. Specifically, OBIM scans copies of the fingerprint cards, uploads them into EAGLE, and then uses EAGLE to query IDENT to find the subjects' FINs. OBIM FOIA then sends the FINs to specific, trained personnel in OBIM's IDENT Operations Unit (OBIM IT personnel devoted specifically to IDENT-related issues) to locate the responsive records (if they exist) associated with each FIN. Those records are then provided to the OBIM FOIA staff to review and then provide the appropriate redress or information to the requesters. The prints used by OBIM to retrieve FINs are retained in EID for 30 days, and then deleted, and prints will not be enrolled in IDENT (unless already enrolled). In addition, OBIM FOIA's access privileges are limited to a search-only capability and the only data retrieved are the FINs, if they exist, associated with each set of fingerprints.

*EDDIE*

ICE developed the EDDIE mobile application so that agents and officers in the field can quickly identify persons encountered during immigration and criminal law enforcement investigations and operations.[3] Specifically, EDDIE assists ICE agents and officers to lawfully collect an investigation subject's fingerprints and photograph using a mobile device, and immediately query other government databases to determine if they contain the same fingerprints as those collected by ICE. Aside from the subject's fingerprints and photograph, EDDIE also collects the PICS ID[4] of the agent of officer who created the entry, transaction information (dates

[2] *See* DHS/ICE/PIA–015(e) EID-EAGLE, July 25, 2012, *available at* www.dhs.gov/privacy.

[3] EDDIE can verify the identity of a subject presumably already known to ICE and is also used to identify a subject who is unknown to ICE by querying other government databases.

[4] *See* DHS/ICE/PIA–013 Password Issuance Control System (PICS), *available at* www.dhs.gov/privacy.

and times when ICE queries other government databases and when the results are returned), and may collect the GPS location where the subject was fingerprinted.[5]

Information collected by EDDIE is stored in EID and can be retrieved using EAGLE. This benefits ICE in two ways. First, it may avoid re-collecting data from the subject during the identification and booking processes. Second, it allows agents and officers in different locations to collaborate on a case. Therefore, if an officer in the field enters data in EDDIE, another officer sitting at his or her workstation can view the information in EAGLE and enter additional data if needed. Likewise, an officer at his or her workstation can enter information in EAGLE, and an officer in the field can view it in EDDIE. ICE Homeland Security Investigations (HSI) agents and Enforcement and Removal Operations (ERO) officers both use EDDIE.

To use EDDIE, users need the following two pieces of hardware: (1) a mobile scanning device to physically scan the subject's fingerprints; and (2) an iOS-based mobile device (*i.e.*, iPhone or iPad). A transaction in EDDIE begins when ICE agents or officers encounter an individual in the field who: is subject to arrest for violation of a criminal or administrative law, based on probable cause; is subject to a brief detention for investigative purposes based on reasonable suspicion that the individual engaged in violation of a criminal or administrative law; or otherwise consents to being fingerprinted. ICE takes the fingerprints of the subject on the mobile scanning device, which then wirelessly transmits the fingerprint images to the user's iOS-based device via Bluetooth.[6] ICE then takes the subject's photograph using the camera feature on the iOS device.

The photographs are not used for the search of IDENT or the FBI's Next Generation Identification (NGI) system.[7] They are collected so that an officer or agent can visually identify one person among a group of people, all of whom had fingerprints collected at nearly the same time, so that returned information can be connected to the correct individual. The photographs are collected by the iPhone within the EDDIE application. Once the full submission is transmitted to the ICE network, the original transaction is erased from the phone. Several pieces of that transaction information are returned to the phone in the form a response, including the photographs, so the officer or agent knows to whom the response applies. All of this takes place within the EDDIE application, which is within a secure container. The photographs are stored in EID temporarily (30 days) unless the subject is booked.

[5] GPS information is not always collected by EDDIE. Rather, the iOS-based device has a setting that allows agents and officers to enable or disable this feature.

[6] As soon as the fingerprint images successfully transfer to the EDDIE mobile application, they are erased from the mobile scanning device.

[7] *See* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis-ngi-biometric-interoperability.

When both the subject's fingerprints and photographs are on the iOS-based device, ICE uses EDDIE to query[8] the Federal Bureau of Investigation's (FBI) Next Generation Identification (NGI) system for criminal history information and IDENT for the subject's immigration history.[9] Upon receipt, NGI and/or IDENT send a response to EDDIE indicating whether there is a fingerprint match (commonly referred to as a "hit") with the subject. ICE generally receives a response within 30-60 seconds indicating whether or not there is a "hit."

A response indicating a positive "hit" in IDENT will not only include the existence of a match, but also the "hit level" (based on the presence or absence of derogatory information pertaining to the investigation subject). IDENT also includes the following information about the subject, if available:

- Name;
- Alien Registration Number (A-number);
- FIN;
- FBI Number; and
- A list of previous immigration encounters and corresponding details.

Unlike information collected by ICE for the biometric identification transaction, information from the IDENT response is not automatically stored in EID; ICE users must manually enter this information in EAGLE to be stored in EID.

The NGI response includes a list of potential candidates who may match the prints submitted by EDDIE. NGI also provides the candidate's Identity History Summary (IdHS), formerly known as a "rap" sheet. The IdHS contains the subject's criminal history and basic biographic information (*e.g.*, name, alias, date of birth). The IdHS is stored in EID for 24 hours before it is wiped from the system. After 24 hours, users must run a new query to receive the IdHS.

ICE officers and agents take follow-up action on an investigation subject based upon the totality of the circumstances presented, including the responses from NGI and IDENT. For example, if both NGI and IDENT indicate that there is a negative response ("no hit") on the subject, there may be other evidence to support continued detention. EDDIE automates what was previously a manual and time-consuming process.

[8] All transactions between the EDDIE mobile application and other government databases (NGI and IDENT) take place through the ICE Network.

[9] Querying IDENT only requires prints of the subject's index fingers, while an NGI query requires all ten prints.

*Digital Application for Victim Witness Identification (DAVID)*

DAVID is an application used by ICE HSI to generate photographic line-ups that are presented to victims and witnesses of crimes for identification.[10] Prior to the implementation of DAVID, ICE either conducted live line-ups or created photo line-ups manually by selecting photographs of individuals with similar characteristics to the perpetrator, and asking a victim or witness to select the person who he or she believed to be the criminal. The DAVID tool streamlines this process by leveraging data collected during arrest processing to automate the creation of photo line-ups that victims and witnesses involved in an investigation can use to identify perpetrators.

The DAVID photo line-up tool provides DHS authorized users the ability to generate photographic arrays to be viewed by victims and witnesses involved in an investigation for identification or exclusion of possible subjects of an investigation. When ICE agents and officers encounter an investigation subject, they collect the subject's biographic information and take the subject's photograph, which is entered into EAGLE and then stored in EID. All DAVID users (limited to HSI agents) can pull the investigation subject's photograph from EID as well as five "filler" photographs to complete the line-up. These "filler" photographs are selected because the individuals have many of the same characteristics as the investigation subject.

DAVID does not automatically search for photographs of individuals with similar characteristics to the subject. Rather, DAVID users use a set of selection screens to input certain physical and biographical characteristics of the subject, such as: height, weight, hair color, age range, and gender. DAVID will then return candidate photos for individuals that are similar based on the agent's input. The physical characteristics used to select photographs are defined by existing EID data sets. DAVID does not use facial recognition to identify similar photographs, but instead relies solely on the characteristics entered by the agent. The other individuals whose photographs are used in the photo array are those who have been arrested by law enforcement officers within DHS or are amenable to immigration removal proceedings. These photographs are pulled from existing entries already in the EID subset of data within IDENT.

DAVID users can re-run the photo array to display a different arrangement of the photos but cannot change the photos themselves. DAVID does not return any additional PII besides the photographs. The photo array that DAVID produces is first shown on the screen, and agents then print a PDF copy of the line-up. This PDF copy is stored in the agent's case file, as the DAVID tool does not store information. HSI agents then present victims and witnesses with a hard copy of the PDF photo line-up to identify the subject.

[10] As explained below, the photographic line-up can also be used to exclude certain individuals as being potential investigation subjects.

If a witness recognizes one of the individuals in the photo line-up, ICE personnel will enter that information into HSI's Investigative Case Management (ICM) system,[11] regardless of whether the witness correctly identified the investigation subject. The photo line-ups also have evidentiary value, as they can be presented to a judge during court proceedings.

*A Typical Transaction in DAVID*

When an HSI agent arrests a subject for either a criminal violation of law or an administrative violation of the INA, he or she will enter the subject's biographic information and data regarding the subject's physical characteristics into EAGLE. The subject's photograph is also entered into EAGLE, and all data pertaining to the subject is stored in EID. DAVID users can then use the tool to create a photographic line-up by using subject records from EID whose physical characteristics match that of the investigation subject.

For example, the investigation subject could be a 42-year-old white male with black hair, weighing 215 pounds. The agent can use DAVID to select other individuals with similar characteristics to use in a photo line-up. From the example above, a DAVID user could filter individuals by querying EID for photographs of white men with black hair, between 35-45 years of age, and weighing between 200-225 pounds. Based on information that had previously been entered into EAGLE, DAVID will pull photographs from EID of individuals who fit the criteria entered by the agent and will create a photo line-up based on these characteristics. The agent then collects these photographs along with the photo of the actual investigation subject and presents a hard copy of the PDF to the victim or witness for identification. The victim or witness then indicates whether or not he or she recognized any particular photograph. HSI stores this information in ICM.

## Reason for the PIA Update

DHS/ICE is updating the 2010 EID PIA to explain OBIM's use of the EAGLE application and to describe two additional applications that use PII collected from investigation subjects: (1) EDDIE collects fingerprints and photographs from investigation subjects using a mobile device; and (2) DAVID creates and displays photo arrays for victims, witnesses, and other individuals to identify possible investigation subjects.

## 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. § 1302(a); 8 U.S.C. § 1324(b)(3); 8 U.S.C. § 1357(a), (c), and (f); 8 U.S.C. § 1360(b); 19 U.S.C. § 1; and 19 U.S.C. § 1509. Additional authority is provided in 6

[11] *See* DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), available at www.dhs.gov/privacy.

U.S.C. § 202; 8 U.S.C. §§ 1365a, 1365b, 1379; 19 U.S.C. §§ 2071, 1581-1583, 1461; and the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

### System of Records Notice (SORN)

The DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN applies to the information collected and maintained by EID.[12] The DHS/ICE-009 External Investigations SORN applies to the information that HSI agents enter into the DAVID application.[13]

### System Security Plan

A system security plan has been completed for EID. EID and its applications go through a system security certification and accreditation process that reviews the security mechanisms and procedures that are in place, and ensures they are operating in accordance with established policy. The Authority to Operate for EID expires on July 21, 2019.

### Records Retention Schedule

Biographic and biometric information maintained in EID falls under Records Control Schedule DAA-0563-2013-0006.[14] 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 after 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.

HSI personnel enter certain information pertaining to the photo line-up process in ICE's Investigative Case Management system (ICM). Specifically, HSI indicates whether a victim or witness identified any photograph(s) in the line-up. Currently, DHS Headquarters (HQ) has a pending Investigative Records schedule, DAA-0563-2018-0002, which will cover investigative case records maintained in ICM. Until there is a records schedule approved by the National Archives and Records Administration (NARA), the investigative case records are covered by U.S.

[12] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, October 19, 2016, 81 FR 72080. The CARIER SORN has replaced what was formerly known as the ENFORCE SORN and is available at www.dhs.gov/privacy.

[13] *See* DHS/ICE-009 External Investigations, January 5, 2010, 75 FR 404, *available at*: www.dhs.gov/privacy.

[14] The retention schedule can be found here: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0001_sf115.pdf.

Customs Legacy schedule, N1-36-86-1.[15] With the exception of munitions control cases, which are permanent, records maintained in ICM are retained for 20 years.

### Characterization of the Information

*EAGLE*

There are no changes to the information collected by EAGLE.

*EDDIE*

EDDIE may collect the following information:

- Fingerprints of the investigation subject;
- Photograph of the investigation subject;
- Subject's capture location (GPS information allowing ICE personnel to confirm the location where an individual was fingerprinted);[16] and
- Identifying information about the agent or officer who created the entry.

All information listed above is stored in EID and retrievable in EAGLE.

Information returned to EDDIE from IDENT and NGI may include the subject's name, A-number, FIN, FBI number, and immigration history. These responses are neither collected by EDDIE nor stored automatically in EID. Rather, relevant information from the NGI and IDENT responses must be manually entered by ICE users into EAGLE for storage in EID. Additionally, the IdHS returned from NGI is only available in EID for 24 hours. If ICE wants to retrieve the IdHS after 24 hours, it must run a new query of NGI. However, after confirming the subject's identity, ICE users can manually enter relevant information from the subject's criminal history from the IdHS into EAGLE so that it is stored in EID for the entire retention period.

Biometric information contained in EDDIE is collected directly from the investigation subject, thereby increasing the likelihood that it is accurate. Because there is a risk that an investigation subject may not be truthful about his or her identity, EDDIE users collect biometrics directly from the subject. Collecting biometric information ensures that ICE has properly identified the individual. Before ICE takes any immigration enforcement action against an individual, ICE personnel run additional searches and conduct interviews so that the subject's record is as complete and accurate as possible. The data points collected by EDDIE (listed in the bullets above) are stored in EID (and therefore retrievable through EAGLE) as soon as they are received by the ICE

[15] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf.

[16] This is not a required field. The capture location will only be collected if Location Services are enabled on the iOS device.

network. EID system administrators ensure the accuracy of the data as outlined in the original EID PIA.

**Privacy Risk:** There is a risk that EID could contain inaccurate data if an EDDIE user makes errors when manually entering information from an IDENT or NGI response into EAGLE.

**Mitigation:** EDDIE users do not enter information into EAGLE regarding an investigation subject until they have confirmed the subject's identity. When EDDIE users receive responses back from NGI and IDENT, they are trained to only consider information pertaining to the data subject and to ensure that the data being entered into EAGLE is accurate. All information is reviewed by a supervisor before it is formally stored in EID. This reduces the risk that information contained in the system will be inaccurate.

**Privacy Risk:** There is a risk that EID contains information about individuals whose information should not be in the system, as NGI could return information on multiple subjects.

**Mitigation:** EDDIE users only enter relevant pieces of a candidate's IdHS into EAGLE after confirming the subject's identity. In the event there is an NGI response with multiple candidates, it is the responsibility of an ICE agent or officer to make a determination about which IdHS applies to the investigation subject. If ICE personnel have questions about the subject's identity, they will run additional searches to confirm. This risk is also mitigated because any IdHS that NGI returns to EDDIE is deleted from EID within 24 hours. In the event that an NGI query returns more than one IdHS, EDDIE users can review the information and are trained to only enter information into EAGLE that matches the investigation subject. Any information entered into EAGLE may be auto-populated onto certain immigration forms, which must be approved by a supervisor. If ICE personnel need an updated IdHS, they must submit a new query to NGI.

*DAVID*

The DAVID tool itself does not collect any PII. Rather, DAVID uses photographs that are already stored in EID to create a hard copy photo line-up so that a victim or witness can properly identify an investigation subject. As discussed above, DAVID users enter certain physical characteristics related to the investigation subject (*e.g.*, hair color, eye color, weight). EID then uses these criteria to generate a line-up of individuals with similar characteristics. All of the information in DAVID comes from EID, which is subject to several levels of review in order to ensure the accuracy of the information, as outlined in the original EID PIA.

### Uses of the Information

*EAGLE*

DHS OBIM uses EAGLE solely to query IDENT to determine an individual's FIN. This allows OBIM to verify an individual's identity by matching the FIN with the fingerprints on the fingerprint card. The OBIM FOIA Division can then appropriately respond to their own FOIA requests that relate to a particular individual.

**Privacy Risk:** There is a risk that OBIM personnel will use EAGLE for purposes beyond what is described in this PIA.

**Mitigation:** EAGLE incorporates user roles and access controls so that only users with a need to know can access specific portions of the system. As explained above, OBIM personnel who use EAGLE to find an individual's FIN are limited to a "search-only" query of IDENT. Therefore, OBIM personnel are unable to edit or alter any PII or other data maintained in the system, helping to mitigate any risk of poor data quality or data inaccuracy. Finally, EID's audit capabilities allow system administrators to track actions such as modifying records, extracting information from the system, and determining which users viewed particular records. This helps to promote accountability of actions taken within the system.

*EDDIE*

ICE HSI agents and ERO officers use EDDIE in the field to quickly identify individuals who are encountered during law enforcement interactions. Agents and officers perform this task by using a mobile scanning device to collect the fingerprints of the investigation subject. EDDIE users may choose to only collect the left and right index fingerprints (sufficient to run a search in IDENT) or all ten prints to run a search in NGI and IDENT. As each fingerprint image is collected, it is transferred to the EDDIE application on an iOS-based device via Bluetooth. ICE agents and officers can then query NGI and/or IDENT to determine if there is a "hit" on the subject based on the fingerprint image. These systems will return a "hit" if the fingerprint images contained in their systems matches the fingerprints in EDDIE. If there is no match, EDDIE will receive a notification of "no hit." This identifying information allows ICE agents and officers to take appropriate action regarding the subject.

*DAVID*

DAVID is used only by ICE HSI agents; ERO officers do not use the DAVID tool. HSI agents use this tool to create a photo line-up for victim and witness identification. When HSI agents encounter an investigation subject, they enter the subject's biographic information, such as name, height, weight, age, gender, hair color, and eye color, into EAGLE, and the data will be stored in EID. Agents then use a set of selection screens to input certain physical and biographic characteristics matching those of the subject. DAVID will then search EID to provide five additional photographs (in addition to the subject's photograph) to be used in the line-up for identification. DAVID provides no PII besides images of individuals who were previously arrested by ICE. Once DAVID compiles the six photographs (the investigation subject and five "fillers"), the compilation will appear as a PDF and is assigned an ID number prior to printing. Agents then present victims and witnesses with a hard copy of the PDF as a photo line-up for identification.

Once the PDF is printed, it is stored in the HSI agent's case file. The photo line-up it is not saved in the DAVID application.

**Privacy Risk:** There is a risk that DAVID users will compile biased photo line-ups by using photographs that do not align with the physical characteristics of the investigation subject.

**Mitigation:** This risk is mitigated because it is in ICE's best interest to create photo line-ups in which the "filler" photographs use the same characteristics as the investigation subject. If the validity of the line-up were to be challenged in court, it may be ruled invalid if the "filler" photographs used individuals of a different gender, a significantly different weight or age range, or a different hair color. Furthermore, the confidence level of the line-up is heightened if a victim or witness can positively identify the investigation subject out of a photo line-up in which all the photographs show individuals with the same physical characteristics.

### Notice

*EAGLE*

ICE provides notice of the new use of EAGLE with the publication of this PIA and the CARIER System of Records Notice (SORN). As a law enforcement agency, ICE does not provide formal notice to subjects of enforcement actions. 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 subjects are aware they are being interviewed by a law enforcement officer and that their information is being collected for use in an investigation.

*EDDIE*

ICE agents and officers use EDDIE to capture an individual's fingerprints and photograph. ICE personnel query NGI and IDENT by submitting the subject's fingerprints to properly identify the individual. ICE personnel receive this information directly from the data subject and verbally inform the individual being fingerprinted that the action is for law enforcement purposes, enforcement action, or in furtherance of a law enforcement operation, thereby ensuring that encountered individuals are put on notice that their information is being collected during a law enforcement investigative encounter. ICE also provides further notice to investigation subjects through the publication of this PIA and the CARIER SORN. Routine uses in the CARIER SORN indicate how DHS may share this information with external third parties.[17]

[17] ICE recognizes that under Executive Order 13768, federal agencies are no longer able to extend Privacy Act protections to non-U.S. persons. However, DHS Privacy Guidance Memorandum 2017-01 (referenced below)

Also, as a law enforcement agency, ICE does not provide formal written notice to subjects of pending enforcement actions. 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.

*DAVID*

DAVID itself does not collect any information directly from the investigation subject. Rather, DAVID pulls photographs previously stored in EID for the purpose of creating a photo line-up for witness identification. Therefore, the source system EID is responsible for providing notice to any affected individuals, when possible. This PIA and the CARIER SORN serve as public notice of how ICE uses the DAVID application.

**Data Retention by the project**

*EAGLE*

The original PIA for EAGLE 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 EAGLE is now retained in EID for 75 years after the end of the calendar year in which the information is gathered.

*EDDIE*

Fingerprints and photographs collected using the EDDIE mobile application are retained in EID for 30 days. After that time, they are purged from EID, unless the subject is enrolled and booked using EAGLE. If the subject is enrolled and booked through EAGLE, the records are maintained for 75 years, after which they are destroyed. Maintaining these records for 75 years allows ICE to compile statistical reports as well as conduct long-term trend analysis. Finally, when ICE personnel use EDDIE to query IDENT and NGI, these databases return information that may be entered into EAGLE and stored in EID. The actual response from NGI (the IdHS) is stored in EID for 24 hours before it is deleted. The response from IDENT (aside from the identifying numbers discussed above) is not stored in EID.

instructs components to balance the public interest against the privacy rights of the individual before making disclosures of an individual's PII. Routine uses published in ICE's SORNs are a result of such balancing, and provide guidance to ICE operators regarding when PII can be shared with third parties. As ICE's disclosure needs evolve, ICE stakeholders reassess or perform additional balancing analyses to update routine uses, thus retaining their reliability as guidance for operators.

*DAVID*

The DAVID tool itself does not retain any information or photographs. All information, including the PDF photo line-up and assigned ID number, are maintained in EID. Photographs of investigation subjects collected during the encounter, arrest, or booking of the subject are stored in EID for 75 years. This retention period not only permits ICE agents and officers to compile statistical reports and conduct long-term trend analysis, but also allows authorized ICE personnel to access a wide array of photographs when assembling the photo line-up.

ICE has not identified any new risks related to data retention, as ICE has decreased the retention period for EID data from 100 years to 75 years. This updated retention period not only allows ICE to evaluate and analyze an individual's encounter history with ICE for the lifetime of the subject, but also lessens the chance of a privacy incident because the data is being kept for a shorter time.

### Information Sharing

*EAGLE*

OBIM uses EAGLE to query IDENT to determine an individual's FIN for identity verification purposes in order to respond to FOIA requests received by OBIM. OBIM does not extract information from EAGLE for response to the FOIA request. OBIM does not share any information obtained from EAGLE outside the Department.

*EDDIE*

EDDIE is used by authorized ICE agents and officers with a valid need to know. EDDIE is not accessible to any external third parties. When ICE personnel collect the fingerprints of investigation subjects, they use these prints to query NGI and/or IDENT.[18] These IT systems then return information regarding the investigation subject to EDDIE. ICE personnel manually enter the data from EDDIE into the subject's EAGLE record, if appropriate. Once the subject's information is entered into EAGLE, it is stored in EID. All information sharing is consistent with the purpose of the system as well as applicable routine uses in the CARIER SORN.

*DAVID*

The DAVID photo line-up application is used only by HSI agents to prepare a photographic line-up so that a victim, witness, or other individual can attempt to identify the investigation subject. These line-ups are saved in PDF format and presented to the witness for identification. PDF versions of the line-up may also be shared with local, state, federal, territorial, and tribal courts (and judges) for evidentiary purposes. If the line-up is used as an exhibit in a court

[18] NGI was formerly known as the Integrated Automated Fingerprint Identification System (IAFIS). The original EID PIA documents how ICE can share fingerprints with the FBI.

proceeding, during discovery, or in settlement negotiations, the information will also be available to opposing counsel, other parties to the proceeding, witnesses, and members of the jury. These line-ups contain only the relevant photographs, and do not include any other PII. The information sharing described here is consistent with applicable routine uses in the CARIER and External Investigation SORNs.

**Privacy Risk:** There is a risk that ICE could share data 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 external third parties who all have a verifiable need to know the information. For example, DAVID users share a PDF of the photo line-up so that the victim or witness can identify the subject of an investigation. Without this information, the victim or witness could not properly make an identification. After the photo line-up is reviewed, it is then returned to the HSI agent and retained for the appropriate retention period. Also, if the validity of the line-up were to be challenged in court, ICE would also share the contents of the photo line-up with the appropriate court, opposing counsel, the jury, and other parties to the proceeding. All information from EAGLE, EDDIE, or DAVID shared outside of DHS is done so in accordance with the routine uses in the CARIER and External Investigations[19] SORNs and as required by law.

## Redress

The right to request access to and amendment of records under the Privacy Act of 1974 (5 U.S.C. § 552a) is limited to United States citizens and lawful permanent residents. Executive Order 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."[20] This Executive Order precludes DHS from extending such rights by policy. However, 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.[21]

[19] The DHS/ICE–009 External Investigations SORN only applies to information that ICE HSI personnel enter into ICM in relation to the photo line-up process.

[20] The full text of Executive Order 13,768 can be found here: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[21] 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.

As a result of Executive Order 13768, DHS's "Mixed Systems Policy"[22] was rescinded by the DHS Privacy Office in its Privacy Policy Guidance Memorandum (April 25, 2017).[23] However, DHS will consider individual requests to determine whether or not an individual may access or amend records contained in this system. Individuals seeking access to and notification of any records contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE FOIA Officer. Individuals who wish to contest the accuracy of records in the system may submit these requests to the ICE Privacy Division.

In addition, the DHS Privacy Policy Guidance Memorandum makes clear that DHS has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes. Failure to maintain accurate records serves to undermine efficient decision making by DHS personnel, and can create the risk of errors made by DHS and its personnel. Also, PIAs are published, in part, to ensure that projects, programs, and systems maintain accurate data.

ICE has not identified any new risks related to redress.

### Auditing and Accountability

All EAGLE, EDDIE, and DAVID users must complete annual, department-wide privacy and security trainings that discuss the proper handling of PII. EID users also complete system-specific training to certify that they know how the system operates and that they can properly handle the information contained within the system.

EDDIE is a mobile application used to lawfully collect fingerprints and photographs, in a standard, law enforcement process. Agents and officers are also trained on reading responses from IDENT and NGI to understand the data provided by these systems. This ensures that the data is accurate, and that ICE takes the appropriate enforcement action against the individual. In addition, EDDIE collects a very limited amount of information directly from the investigation subject in accordance with the fair information practice principle of data minimization.

[22] 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, as well as 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.

[23] 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.

EID maintains audit logs of user activity to allow system administrators to monitor user behavior in the system. Audit logs will track when individuals are logged into the system, who views which records, and how records are used within the system. If system administrators notice that anyone has used the system in violation of ICE policy, the user may be disciplined in accordance with appropriate ICE policies.

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) must be completed and signed by the supervisor. The roles and privileges assigned to a specific user depend on that user's job responsibilities. EID and the applications that write to EID further restrict users' access to specific functions based on the role assigned to them. The assigned user role determines which 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 system administrators only.

## Responsible Official

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

## Approval Signature

[Original signed and on file with the DHS Privacy Office]

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security