Privacy Impact Assessment Update
for the

Enforcement Integrated Database (EID)
Criminal History Information Sharing (CHIS) Program

DHS/ICE/PIA-015(h)

January 15, 2016

Contact Point
Peter Edge
Executive Associate Director, Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

Since 2010, U.S. Immigration and Customs Enforcement (ICE) has shared certain criminal history information with foreign countries concerning nationals of those countries who are being repatriated from the United States and who were convicted of certain felonies in the United States. This information sharing effort is referred to as the Criminal History Information Sharing (CHIS) program and is formalized by cooperation agreements between DHS and each participating country. ICE shares the information provided through the CHIS program from the Enforcement Integrated Database (EID), which 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 ICE and U.S. Customs and Border Protection (CBP). The CHIS program began in 2010 with the United Mexican States and has since expanded to other nations. It has been documented in various updates to the Privacy Impact Assessment (PIA) for EID, which was originally published in January 2010.[1] This update to the EID PIA describes a change to the CHIS program whereby ICE will use a secure web service to share this criminal history information with its foreign partners.

Introduction

EID is owned and operated by ICE and supports the law enforcement activities of certain DHS Components. EID is the common database repository for all records created, updated, and accessed by a number of software applications including the EID Arrest Guide for Law Enforcement (EAGLE) and the ENFORCE Alien Removal Module. Collectively these applications are referred to as the "ENFORCE/EAGLE applications." EID and the ENFORCE/EAGLE 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 CBP. EID provides users with the capability to access a person-centric view of the data using the ENFORCE/EAGLE applications. Users can also print reports, notices, and other documents containing EID data, which are used for criminal and administrative law enforcement purposes and typically are retained in criminal investigative files, detention files, and 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 before U.S. immigration courts. Forms and data may also be provided to the criminal courts of the United States.

[1] The EID PIA and PIA Updates documenting the CHIS program are as follows: DHS/ICE/PIA-015(a), DHS/ICE/PIA-015(c), and DHS/ICE/PIA-015(f), *available at* http://www.dhs.gov/privacy-documents-ice.

The PIA for EID, published in January 2010, describes EID and the ENFORCE applications, and reflects the system at that time. DHS published a number of PIA updates describing changes to the EID systems including the establishment of the CHIS program, which was originally limited to sharing with Mexico. DHS later expanded the scope of external sharing of EID information beyond the Government of Mexico to multiple foreign partners.[2]

DHS also expanded the CHIS program's criminal history sharing to include biometric information (photographs and fingerprints). Photographs shared by CHIS are obtained from EID. DHS Automated Biometric Identification System (IDENT) stores fingerprints on behalf of ICE and other DHS component agencies. CHIS shares fingerprints from IDENT with foreign partners. In addition, the expansion also allowed for ICE to receive reciprocal criminal history information from its foreign partners for foreign nationals being removed from the United States.[3] Inclusion of biographic and biometric information sharing for non-criminal removable aliens was initiated with the CHIS agreements for all foreign partners except Mexico.

Reason for the PIA Update

DHS shares EID information with its foreign partners to coordinate and conduct the removal of foreign nationals from the United States. The current method of data sharing is a manual process whereby an ICE officer or agent emails the encrypted biometric and biographic data to the appropriate foreign partner. This update provides notice of ICE's implementation of a new method to transmit this information to its foreign partners via a web service to enable automated processing. The new method of sharing will consist of a secure CHIS web service hosted in the ICE Demilitarized Zone (ICEDMZ) environment as detailed in the Technology section below. The CHIS web service has been designed in a way that allows ICE and its foreign partners to maintain their network integrity while enabling the sharing of this sensitive Law Enforcement data.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

ICE is establishing a new web service to facilitate the automated sharing of information between the United States and participating foreign partners. This change will affect sharing with those foreign partners capable of developing the infrastructure necessary to send and receive an automated feed with the ICE web service.

---

[2] *See* DHS/ICE/PIA-015(f) for foreign partners with whom DHS plans to enter into CHIS agreement with in the near future.
[3] *See* DHS/ICE/PIA-015(f), April 8, 2014.

The information collected and stored within EID will not change with this PIA update. EID will continue to maintain information that is collected and used by the ENFORCE/EAGLE 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. The personally identifiable information (PII) maintained in EID will continue to consist of biographical, descriptive, biometric, and encounter-related data about subjects and includes name(s), alias(es), date of birth, telephone numbers, addresses, nationality, citizenship, Alien Registration Number (A-Number), Social Security number (SSN), passport number, visa information, family history, employment history, educational history, immigration history, and criminal history.

Privacy Risk: There is a minimal privacy risk that the automated service may not accurately identify the individuals whose data is to be shared under the CHIS agreements.

Mitigation: CHIS only selects individuals who are nationals of a foreign partner with a Final Order for Removal in the ENFORCE Alien Removal Module (EARM). Individuals without a Final Order are not selected by CHIS for inclusion in the CHIS transmission. Once CHIS selects an individual with a Final Order, CHIS populates specific data fields in the manifest that will be shared with the relevant foreign partner.

In the very unlikely event an individual has an incorrect final order status and his or her information is transmitted, ICE will correct the status in the system and initiate direct communication with the foreign partner to have the information deleted from the foreign partner's records.

Privacy Risk: There is a risk that the automated service might share incorrect data fields or elements.

Mitigation: In order to mitigate this risk, the CHIS web service is implemented as an automated programed system that extracts data from EID in the same manner each time. As an automated program this reduces the risk of human interference and provides a degree of technical control over the process. The program will identify the correct individuals who meet the requirements for information sharing, as well as control the data fields that are shared with ICE's foreign partners.

The CHIS web service was designed to meet the requirements spelled out in the cooperation agreements and is tested extensively prior to each release. This testing includes automated testing as well as manual testing with detailed reviews of the test results. The review validates that information will only be shared for those individuals who meet the CHIS requirements and only those fields identified as being eligible for sharing are included in the transmission. The fields are currently limited to: A-Number, Subject ID, name, alias, date of birth, city of birth, country of birth, mother's name, father's name, gender, gang flag,

photographs, fingerprints, National Crime Information Center (NCIC) Code(s) from the 85 crimes enumerated in the cooperation agreements, description of crime, and date of conviction.[4]

Uses of the System and the Information

Uses of the system and the information are not changed with this PIA update. ICE will continue to externally share criminal history and biometric information from EID with foreign partners relating to those foreign partners' nationals who are being removed from the United States. Reciprocally, ICE's foreign partners will continue to share criminal history information with DHS for these same nationals who have been convicted of similar or equivalent felonies in the foreign partners' country, and ICE will enter this information into the alien's EID record.

DHS will continue to enter into legally non-binding cooperation agreements with its foreign partners to formalize CHIS agreements. The intent of these agreements is to limit the use of shared criminal history information for authorized purposes and to prevent public or third-party disclosures unless authorized by the participant country that provided the information. Participants agree to implement and maintain specified security measures such as: background screening of personnel and restricted access; physical and technical security of terminals and telecommunications lines; data security; data dissemination; logging and audit procedures; and notification of reported suspected or actual unauthorized access. Each party will retain the right to suspend, modify, or terminate participation. In the event the agreement is suspended or terminated, data transmissions would terminate and data that has already been transmitted will be handled according to the agreement in place at the time of the transmission.

Retention

This PIA update does not change the retention period for information maintained in EID.

Internal Sharing and Disclosure

Internal sharing and disclosure of EID information is not changed with this PIA update.

External Sharing and Disclosure

Regardless of the method of sharing (email or web service), the exact data items are shared in identical Extensible Markup Language (XML) record format. The method of sharing criminal history and biometric information from EID will only change for those foreign partners

[4] *See* DHS/ICE/PIA-015(f) Enforcement Integrated Database, April 8, 2014 for more information about the CHIS agreements.

that elect to participate in the web service. Please see a detailed discussion of the web service in the Technology section below. For those that do not participate in the web service, the method of sharing will continue to occur via email. The types of data being shared will not change. ICE will continue to share EID information with its foreign partners to coordinate and conduct the removal of foreign nationals from the United States. The following information will be shared from EID: A-Number, Subject ID, name, alias, date of birth, city of birth, country of birth, mother's name, father's name, gender, gang flag, photographs, fingerprints, NCIC Code(s) from the 85 crimes enumerated in the cooperation agreements, description of crime, and date of conviction.

Notice

ICE shares information with foreign partners in accordance with the DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE) System of Records Notice (SORN), routine use M.[5] Routine use M states that ICE may disclose information to foreign governments for the purpose of coordinating and conducting the removal of aliens to other nations; and to international, foreign, and intergovernmental agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

Individual Access, Redress, and Correction

This PIA update does not change the ability of an individual to access, redress, and correct his or her information.

Technical Access and Security

There is no change to the technical access and security of EID.

Technology

Under existing CHIS program procedures, ICE officers or agents currently send EID information, described above, via encrypted email attachments to the foreign partners. The emails contain two attachments, one attachment of EID information formatted to be read by a law enforcement official and a second attachment (containing the same information) in a format designed for ingestion into the foreign partner's database. The attachments are sent to a secure email account with the foreign partner's designated law enforcement agency. This method of sharing will continue; however, a new method of sharing, described below will also be available.

[5] DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE), 80 FR 24269 (April 30, 2015).

With this PIA update, ICE will add an additional option for information sharing with foreign partners via a web service. The information shared via the web service will include the same EID and IDENT information described above for criminal aliens who are being removed from the United States and who have been convicted of certain firearms, national security, violent, and drug-related felonies.This same EID biographic and IDENT biometric information, minus references to historical criminal encounter information, will be shared for all aliens who are arrested for administrative violations of the Immigration and Nationality Act (INA), have a final order of removal, and have no pending appeals for that final order.

The automated CHIS data transfer mechanism is comprised of a number of loosely-coupled, secure web services implemented both inside the ICE firewall and in the ICEDMZ. A loosely-coupled design reduces the inter-dependencies between operational functions of the system with the goal of reducing the risk that changes in one aspect pof the system will necessitate changes in other functionality of the system. The ICEDMZ environment is an area separated and located outside of ICE's internal network, but still under the control of the agency. ICEDMZ is protected by a firewall and on a separate, isolated ICE network. This area is located between ICE's internal environment and the foreign partners' internal environment. This configuration allows for the protection of each entity's network, as the exchange of information takes place outside of their respective firewalls.

The use of the web service is available to all foreign partners, and will enable automated processing by foreign partners capable of developing the infrastructure to handle the automated feed. Each foreign partner will develop its own web service application to access the CHIS web service based on standardized protocols provided by ICE. Once a foreign partner has developed its web service application to connect to CHIS, the CHIS web service will authenticate its application based on two-factor authentication and use Secure Socket Layer (SSL) encryption. This will establish a secure connection to enable the safe transfer of information between the ICEDMZ environment and the foreign partner.

The CHIS web service first positively confirms the identity of the foreign partner using a combination of SSL technology and Authentication, Authorization, and Accounting (AAA) protocol, then serves the information to the foreign partner in the same XML format contained in the current manual email transmission method. SSL uses key cryptography to establish a link between the CHIS web service and the foreign partner. This link provides for the secure transfer of information via email and web service between the two entities. The AAA protocol will authenticate the foreign partners, control access to the system's resources, audit usage, and track the user's activities. Once the CHIS web service has validated the foreign partner's credentials, CHIS will transmit data to the foreign partner.

CHIS does not store or retain information after a successful transmission. The process is designed to retain data only as long as needed to support the transmission of information. Once the foreign partner confirms receipt of the data from the database, the system is programmed to

automatically delete the data from the encrypted database within ICEDMZ. The date and time of the transmission will be stored for auditing and troubleshooting purposes.

Outbound: From CHIS to foreign partners

The process begins when the CHIS application identifies an individual with a new final order for removal. The CHIS application sends information about one individual at a time to simplify the validation, transmission, and receipt. The application gathers the relevant information regarding this individual and sends a message to a secure encrypted database in the ICEDMZ. This information will be shared with the foreign partner. When foreign partners want to retrieve the information from the encrypted database, the foreign partners' application will call the CHIS web service with a 'RETRIEVE' command.

The CHIS application will determine the transmission method requested by the foreign partner and send the XML-formatted record either via automated encrypted email or web service. If sent via email, the lists' destination is a designated, foreign partner government email address, with limited access and vetted by ICE OCIO. If the transmission method is via web service, the lists' destination is the encrypted database in ICEDMZ. The data will stay in the encrypted database in ICEDMZ until the foreign partner calls the CHIS web service in with a 'RETRIEVE' command.

The foreign partner receives the same data in the same XML format regardless of the transmission method. The benefit of automated web service transmission over a manual process is that human interaction is removed. Removing human interaction decreases the response time and reduces data entry errors. Further, the use of the web service enables automated searching and vetting of foreign nationals in the foreign partners' system, potentially reducing the time needed to screen and/or identify persons of interest.

Inbound: From foreign partners to CHIS

Foreign partners will continue to the have the option of sharing biographic and criminal history information with ICE, via email or the web service. The information shared will pertain to the same aliens that ICE has deported to the foreign partners' country. The same data is returned to ICE in the same format regardless of which method is chosen. The advantage of using the web service is that human interaction may be removed from this process thereby speeding the response and reducing data entry errors. If the web service transmission is chosen, the foreign partners will call the CHIS web service with a 'POST' command to place the data in the encrypted database in ICEDMZ. The CHIS service will validate the foreign partner's credentials, validate the content of the message, store the data in the encrypted database, and respond to the foreign partner with a successful status. Once a foreign partner shares information in the encrypted database in the ICEDMZ, ICE will send the information to the ICE exchange

service and email the information to the Criminal Alien Program. The Criminal Alien Program will manually review the information and insert the data into EID. This process is currently in place and will continue.

At a later date in CHIS version 1.15, no emails will be sent to the Criminal Alien Program. The CHIS application will make periodic 'RETRIEVE' calls to the CHIS web service to import the foreign partners' data from the encrypted database in the ICEDMZ and move it inside ICE's internal network. The data received from the foreign partner will be vetted before the information is placed into EID. When data is retrieved from the CHIS web service, the data will be passed to the Crime Entry Screen (CES) application. CES is an ICE application used by EARM to enter an alien's criminal history information into EID. The CES application will perform a lookup function in EID to locate the alien's information. An immigration officer will review the information in EID and compare it to the data from the foreign partner. Once the data is verified and in the correct format, the data will be ingested into EID.

Email delivery of biographic and criminal history information from foreign partners to ICE may continue on a country-by-country basis, until web service delivery is established with all participating foreign partners.

Privacy Risk: There is an increased risk of unauthorized access to the data if the connection between systems is not properly designed. Security failures could compromise the connected systems and the data that they store, process, or transmit could be compromised or disclosed.

Mitigation: The CHIS web service was designed with architecture to support the security of both the ICE network and the networks of ICE's foreign partners. This design enables each entity to maintain network integrity by not allowing any foreign element to reach inside its network or push data inside its network.

The data is placed in ICEDMZ and each participant goes outside of its internal network to get the data when it is ready. Placing the data in the ICEDMZ allows for data validation before the information is stored inside a foreign partner's network. By implementing the services in the ICEDMZ environment, ICE can control the firewalls between ICE and the ICEDMZ as well as between ICEDMZ and its foreign partners. In addition, ICE controls the installation and maintenance of the SSL certificates required for foreign partners' connection and validation. Further, ICE mitigates transmission failure by eliminating the need for a direct connection between ICE and its foreign partners. ICE and its foreign partners can POST and RETREIVE information any time their own web service is available. ICE does not need to validate a current, successful connection to a foreign partner before transmitting data. Only a connection to ICEDMZ must be available, which is under the control of ICE.

Privacy Risk: There is also a risk of unauthorized access due to insufficient data security associated with leaving information in the ICEDMZ environment until the foreign partner retrieves the information from the database.

Mitigation: To ensure data security while data resides in the ICEDMZ, the CHIS application employs SSL in conjunction with AAA protocol. Using these transmission protocols together ensures that each piece of data is secure from outside attacks as well as visible only to the proper owner while it is residing in the ICEDMZ. The CHIS application uses table level encryption to protect the data at rest in the ICEDMZ environment, which meets or exceeds all DHS security requirements. In addition, this risk is minimized by the use of cooperation agreements, as described earlier, between ICE and each foreign government that governs the use of the web service.

Responsible Official

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

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security