Privacy Impact Assessment Update
for the

ICE Pattern Analysis and Information Collection (ICEPIC)

DHS/ICE/PIA-004(a)

October 26, 2011

Contact Point

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

Reviewing Official

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

Abstract

U.S. Immigration and Customs Enforcement (ICE) has established a system called the ICE Pattern Analysis and Information Collection (ICEPIC) system. ICEPIC is a toolset that assists ICE law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations that are indicative of violations of the customs and immigration laws as well as possible terrorist threats and plots. The Privacy Impact Assessment (PIA) for ICEPIC was published in January 2008. This PIA Update is being completed to provide transparency related to the Law Enforcement Information Sharing Service (LEIS Service) that enables law enforcement agencies outside DHS to query certain information available through ICEPIC. Additionally, DHS law enforcement personnel are able to query external law enforcement agencies' sensitive but unclassified law enforcement information.

Introduction

ICEPIC was created in 2008 to assist ICE law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations. The information processed by ICEPIC is a compilation of information from existing DHS investigative and apprehension records systems, as well as immigration benefit and alien admission records systems. Today, ICEPIC still compiles information from the same existing systems as described in its original 2008 PIA; no additional systems have been added. [1]

In addition to what is described in the original PIA, ICEPIC data is accessed by external federal, state, local, tribal and international law enforcement agency partners (member agencies) through a web service called the LEIS Service. The member agencies use the LEIS Service as a sharing service to access filtered information from ICEPIC. These member agencies participate in a particular federal, state, local, tribal, regional, or international information sharing service (as described in this Update's Appendix) to extract sensitive but unclassified DHS law enforcement information. The information sharing occurs by extracting the appropriate information from ICEPIC through the use of a Web-accessible service operated by DHS known as the LEIS Service.

[1] Information contained in ICEPIC is detailed in the DHS/ICE/PIA-004 - ICE Pattern Analysis and Information Collection (ICEPIC) System of Records Notice (SORN) located here: http://edocket.access.gpo.gov/2008/E8-19031.htm.

This information sharing through the LEIS Service is authorized by Section 701 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), PL 107-56 (2001 HR 3162). This section of law authorizes the establishment and operation of information sharing systems to enhance the investigation and prosecution abilities of participating law enforcement agencies in accordance with written information sharing Memoranda of Agreement (MOAs) between DHS and federal, state, local, tribal, regional, or international information sharing services providing access to member agencies. DHS signs MOAs with federal, state, local, tribal, regional, or international information sharing services.[2] Various federal, state, local, tribal, and international member agencies participate in these information sharing services. The terms of the MOA are structured to apply to the member agencies accessing information through the information sharing services.

The LEIS Service provides member agencies with access to DHS law enforcement records related to persons of interest, including suspects in child pornography, drug smuggling, immigration fraud, alien smuggling, and in other instances where the member agency has a predicated reason to identify such persons of interest for a criminal law enforcement purpose. Through their own federal, state, local, tribal, regional, or international law enforcement information systems, law enforcement personnel at member agencies can query the LEIS Service to access certain information related to DHS criminal and national security investigations through the use of name and/or identifying number queries. Before the LEIS Service deployed, this type of law enforcement-to-law enforcement information sharing occurred manually through ad hoc queries DHS received from other federal, state, local, tribal, and international law enforcement agencies. The LEIS Service offers a more efficient system for requesting and sharing investigative information, improving the efficiency and automation of information sharing between DHS and its law enforcement partners than previously existed using manual email- and telephone-based information sharing.

What DHS Information Shared is Shared With Member Agencies Through the LEIS Service

While ICEPIC contains a broad range of information from DHS source systems, only a limited subset of that information is made available to member agencies through the LEIS Service. The Appendix to this PIA Update provides greater detail on which information is shared according to the information sharing MOAs and will be updated as new MOAs are signed to provide greater transparency.

How DHS Information is Shared With Member Agencies Through the LEIS Service

To access the LEIS Service, the connecting federal, state, local, tribal, regional, or international information sharing services are modified to permit member agencies authorized

[2] For example, National Law Enforcement Telecommunications System (Nlets),National Data Exchange (NDEx) and , Texas Data Exchange (T-DEx).

law enforcement personnel to query the LEIS Service and display results containing select DHS law enforcement information from ICEPIC. DHS relies upon the existing federal, state, local, tribal, regional, or international information systems to vet and authenticate appropriate users of the LEIS Service. DHS relies on the member agencies to identify appropriate users of the LEIS Service based on the MOA with the information sharing service. The LEIS Service MOAs with the information sharing services do not allow the member agencies' authorized users to store DHS information on the external user's computer or storage media. The information accessed through the LEIS Service is displayed but not stored.

When the member agency conducts a query based on a name and/or identifying number, such as alien registration number, vehicle identification number, I-94, driver's license, or other identification number associated with an individual through the connecting federal, state, local, tribal, regional, or international information sharing service to the LEIS Service, the LEIS Service searches ICEPIC for matching name and/or identifying number records contained in the subset of ICEPIC data authorized for LEIS Service users. If matching records are found, the LEIS Service then extracts the allowable data fields from the matching record and displays it electronically to the member agency user who performed the query.

Member agency users can only conduct single queries based on an individual identifier; the LEIS Service does not allow the user to conduct batch queries or queries of multiple distinct names and/or distinct identifying numbers at one time. The results returned by the LEIS Service typically are subject name, date of birth, and address. If available, the returned hit information may also include height, weight, eye color, and hair color, and country of birth and/or place of birth information as well as, in some instances, person subject photos.

How Member Agencies Use Information Shared Through the LEIS Service

Only federal, state, local, tribal, regional, or international information sharing services that have entered into MOAs with DHS are provided computer connectivity to the LEIS Service. The information accessed through the LEIS Service may be used only for official criminal law enforcement purposes, national or homeland security purposes, and background checks on applicants seeking employment with the member agency. Criminal law enforcement purposes are defined as the investigations of alleged violations of law where DHS or member agencies have the authority to enforce or support the enforcement of the law. National or homeland security purposes are those activities undertaken to identify, prevent, interdict, deter, or disrupt threats to the United States, its people, property, or interests, including threats involving terrorist activity, the use of weapons of mass destruction, and other threats and hazards to the nation where DHS or the member agency has such authority. For background check purposes, the LEIS Service may only be used by member agencies when conducting a background check on applicants seeking employment with the member agency. Finally, member agencies cannot release to third parties any information obtained via the LEIS Service without written consent

from DHS, and the information cannot be used as a substitute for a certified copy of the DHS original record in affidavits filed in a court of law to support law enforcement actions.

How DHS Queries Member Agencies' Data

The LEIS Service allows for bi-directional sharing of data between DHS and the information sharing services. This allows DHS information to be shared with member agencies and allows DHS users to access member agencies' law enforcement data that is entered into the information sharing service, consistent with Section 701 of the USA PATRIOT Act. The LEIS Service allows DHS users (via the ICEPIC system) to query and view, but not store, member agency law enforcement data. This data exchange between DHS and member agencies has been implemented utilizing with the National Information Exchange Model (NIEM) compliant using the LEISP Exchange Specifications (LEXS) 2.0/3.1 data exchange interface. Within DHS, ICEPIC was modified to allow DHS users to query external law enforcement data made available through the LEIS Service. Thus, external law enforcement agencies can provide information through the LEIS Service to DHS.

Privacy Risks and Mitigations

Based on the above described updates to the ICEPIC system, there are three main privacy risks. The first privacy risk relates to the lack of consistency between the existing ICEPIC PIA published in 2008 and the sharing practices of the LEIS Service, which have been operational since 2008 but were not disclosed in public privacy documentation. The first privacy risk is mitigated by the publication of this PIA.

The DHS Privacy Office has taken concrete steps since 2008 to continue to ensure privacy gaps are identified and closed. Specifically, DHS has appointed component privacy officers in all operating components including ICE. The component privacy officer provides ICE and DHS a day-to-day operational level expert who is quickly able to identify privacy risks and mitigation strategies. DHS has improved its process for reviewing updates to systems and programs, via its Privacy Threshold Analysis (PTA) process. The PTA is a tool for program managers to propose program changes to allow the component privacy officers and the DHS Privacy Office to analyze the privacy risks and determine next steps. Additionally, DHS has a policy to review PTAs and PIAs every three years. The systematic review of all PTAs and PIAs every three years provides an opportunity to ensure the privacy compliance documentation accurately reflects the operational program.

The second privacy risk relates to the fact that LEIS Service allows users outside DHS to directly query ICEPIC data that has not been directly reviewed by a DHS employee and therefore could be misinterpreted by external users. This privacy risk is mitigated in two ways. First, as part of the MOA process it is clearly stated that member agencies may not use the responsive data from the LEIS Service query as a substitute for a certified copy of the DHS

original record in affidavits filed in a court of law to support law enforcement actions. If member agencies wish to use the data, they must contact DHS to receive a certified copy. This allows DHS the opportunity to review the request and ensure that the member agency fully understands the context of the information being provided; thereby improving the overall quality of the data being shared. Additionally, the MOA prohibits the member agency from storing the query data or releasing query data to third parties without the written consent from DHS. This ensures that DHS is able to account for how its information is being shared. Second, DHS limits access to the data in ICEPIC to only that which can be shared pursuant to statutory, regulatory, and policy constraints. To limit data access, the information DHS shares via the LEIS Service is a filtered subset of data compiled by ICEPIC, limited to only law enforcement data. Additionally, ICE has created filters on the law enforcement data to ensure that the system controls the amount and type of information being shared. Finally, DHS has limited member agencies' uses of the data to criminal law enforcement purposes, national and homeland security purposes, and background checks on applicants seeking employment with the member agency.

The third privacy risk relates to which users from the member agencies query ICEPIC data through LEIS Service. DHS relies upon the decision of the member agency and the federal, state, local, tribal, regional, or international information sharing service to identify which specific employees should have access to the LEIS Service. To mitigate this risk, DHS has explicitly placed restrictions through the MOA on the purposes for which the information may be queried. Additionally, DHS has audit capability in the event there is a question about a particular user or group of users. Finally, DHS routinely reviews the organizations and as necessary individuals using the LEIS Service; if there is an anomaly DHS will follow up with the organization to identify whether the system is being improperly used.

Reason for the PIA Update

This PIA Update is being completed because the existing ICEPIC PIA does not describe the information sharing that is being conducted through the LEIS Service. The LEIS Service enables law enforcement agencies outside DHS to query certain information available through ICEPIC. Additionally, DHS law enforcement personnel are able to query external law enforcement agencies' sensitive but unclassified law enforcement information.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

The LEIS Service does not collect or store information but is a means by which queries from external law enforcement information systems are run against certain DHS law enforcement records in ICEPIC. The LEIS Service also retrieves any relevant results and delivers those to the querying system for delivery to the user. ICEPIC is a compilation of information from existing DHS investigative and apprehension records systems, as well as immigration and alien admission records systems. However, not all information compiled in ICEPIC is available to member agencies through the LEIS Service. Information that is restricted from disclosure by statute, regulation or policy is filtered and not shared with member agencies. Information available to member agencies through the LEIS Service is limited to certain records as discussed in the Appendix. If member agencies wish to use the data, they must contact DHS to receive a certified copy. This allows DHS the opportunity to review the request and ensure that the member agency fully understands the context of the information being provided.

In many instances, the LEIS Service also allows DHS ICEPIC users to query member agencies' relevant sensitive but unclassified law enforcement databases. ICEPIC users may not incorporate the information from these member agencies' databases without explicit permission via a written certified copy from the member agency.

Uses of the System and the Information

The information provided through the LEIS Service both to member agencies and DHS ICEPIC users may be used for official criminal law enforcement purposes, national or homeland security purposes, and for background checks on applicants seeking employment with member agencies. For example, the information may be used to assist with investigations, to notify requesting officials of past criminal behavior, or to validate a subject's key biographic information. By agreement, DHS information accessed by member agencies through the LEIS Service cannot be accessed or used for any other purpose, including general licensing and eligibility for federal or state benefits.

The LEIS Service is focused on law enforcement partners external to DHS and does not change how DHS users use ICEPIC. As discussed in the introduction, the LEIS Service is designed to provide member agencies query access to specific data elements of certain DHS law enforcement systems. Member agencies query the LEIS Service to determine if DHS has information on specific subjects of interest. Queries from member agencies must contain person information, location information, a telephone number, or an identifier (only one from each type may be included in a query). The LEIS Service then searches ICEPIC for matching name and/or identifying number records contained in ICEPIC. If matching records are found in ICEPIC, the LEIS Service then extracts the allowable information that matches and sends it electronically to the member agency's authorized user. The LEIS Service does not allow member agencies to use

ICEPIC's non-obvious relationship discovery tools or visualization tools. It only offers a query and return capability. The LEIS Service is not used by DHS employees to search ICEPIC, it is only used by external parties to search ICEPIC. DHS employees use ICEPIC directly, consistent with their responsibilities and need to know.

Based on the MOAs (also outlined in the Appendix), certain information sharing services allow ICEPIC users to query their law enforcement databases. These bi-directional MOAs allow ICEPIC to query by name or other personal identifier, but not to retain the data in ICEPIC.

Retention

Responses to queries through the LEIS Service are not retained beyond a specific query session. Responses to queries of external information sharing services through ICEPIC are also not retained by ICEPIC. For example, if ICE requests an official copy of a document found through a connecting information sharing service from the member agency that generated the document, that record will be maintained in one of ICE's official case management systems, such as ENFORCE. Thus, this update does not change the retention period for information maintained in ICEPIC.

Internal Sharing and Disclosure

This update does not change the internal sharing and disclosure of information in ICEPIC.

External Sharing and Disclosure

Only federal, state, local, tribal, regional, or international information sharing services that have entered into the LEIS Service MOA are provided computer connectivity to the LEIS Service. These agreements spell out in detail the terms and conditions of accessing the LEIS Service and the authorizations and limitations for use, disclosure, retention, safeguarding, and destruction of information accessed through the LEIS Service. As noted above, specific provisions in the agreement require that the data queried through LEIS Service be used for specific purposes, that it may not be further transferred beyond the member agency personnel who have direct access to the LEIS Service, and that the data may not be retained unless an official copy is sought and received by the member agency. The MOAs also specify the level of information security of the systems querying ICEPIC and authenticate users. Further, the agreements also spell out the obligations of the member agencies and their personnel for abiding by DHS policies for maintaining privacy with regard to personally identifiable information (PII) contained in the DHS law enforcement records. Specifically, the information may be accessed through the LEIS Service only for official criminal law enforcement purposes, national or homeland security purposes, and background checks on applicants seeking employment with the member agency. The information obtained by member agencies via the LEIS Service may not be accessed or used for any other purpose.

The LEIS Service provides member agencies consisting of federal, state, local, tribal, and international law enforcement agencies query capability to DHS law enforcement records related to persons of interest, including suspects in child pornography, drug smuggling, immigration fraud, alien smuggling and a wide range of other cases. The appendix provides additional specifics on the information sharing and will be updated periodically as MOAs are signed.

Information obtained by member agencies through the LEIS Service cannot be further disclosed by the member agency without obtaining prior written consent from DHS.

Notice

This PIA Update provides accurate information on the current sharing of the information. The System of Records Notice already has an appropriate routine use, and has since it was first published in 2008.[3]

Individual Access, Redress, and Correction

There is no change regarding the access, redress, correction or privacy risks for the ICEPIC system with this update.

Technical Access and Security

Before access to the LEIS Service is granted to an information sharing service, the service must certify to DHS that their users have undergone background checks that require, at a minimum, criminal history and national fingerprint checks. In addition, both the member agencies' system and the LEIS Service have audit capabilities that log the date, time, subject, and originating account of all user queries to the LEIS Service. These audit logs are maintained for five years or for the life of the records accessed, whichever is longer. The results of the audit reports or other internal investigations related to performance under the MOA are shared between the parties upon request.

[3] See footnote 1.

Information provided through the LEIS Service is encrypted during delivery from ICEPIC and the DHS Network to the member agencies' systems. In addition, the LEIS Service validates the registered security certificate of the member agencies' systems to verify the identity of the member agency user prior to sending any information to the user.

Technology

There is no change to the technology of the ICEPIC system with this update. The LEIS Service provides additional capabilities to share certain information with law enforcement entities outside DHS.

Responsible Official

James Dinkins
Executive Associate Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement

Approval Signature

_Final version signed and on file with the Privacy Office.__

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

Memoranda of Agreements for use of LEIS Service of certain ICEPIC data

I. Law Enforcement Organizations with Bi-Directional Query Capability:

- Department of Justice (DOJ): OneDOJ is a repository for DOJ law enforcement components' data that enables internal sharing of investigative information within the Department.
- National Data Exchange (N-DEx): N-DEx is a repository for information from contributing state, local, tribal, and federal law enforcement and criminal justice entities that provides the capability to make potential linkages between law enforcement information contained in crime incidents, criminal investigations, arrests, bookings, incarcerations, parole and/or probation reports in order to help solve, deter, and prevent crimes.
- AZLink (Arizona): AZLink is a collaboration between four regional law enforcement "hub" data centers for the various regions in the state (Central, Eastern, Northern and Southern regions) of Arizona.
- North Central Texas Law Enforcement Analysis Portal (LEAP): LEAP is a data repository that contains information from law enforcement agencies in the states of Texas, Oklahoma and New Mexico,
- Texas Department of Public Safety Texas Data Exchange (T-DEx): TDEx is a data repository containing information from laws enforcement agencies in the state of Texas.
- Law Enforcement Information Exchange Northwest (LInX NW): LInX NW is a data and information sharing network sponsored by the Naval Criminal Investigative Service (NCIS) and the U.S. Attorney's Office for the Western District of Washington state.
- Law Enforcement Information Exchange Hampton Roads (LInX HR): LInX HR is a data and information sharing network sponsored by the Naval Criminal Investigative Service (NCIS) and law enforcement agencies in the Tidewater region of Virginia.
- Law Enforcement Information Exchange North Capital Region (LInX NCR): LInX NCR is a data and information sharing network sponsored by the Naval Criminal Investigative Service (NCIS) and several law enforcement agencies in the District of Columbia, Maryland and Virginia metropolitan area.
- Law Enforcement Information Exchange Southern California (LInX So Cal): LInX SoCal is a data and information sharing network sponsored by the Naval Criminal

Investigative Service (NCIS) and several law enforcement agencies in the southern region of California.

- San Diego Automated Regional Justice Information System (ARJIS): ARJIS is a criminal justice enterprise network that shares information among justice agencies throughout San Diego and Imperial Counties.
- Los Angeles Sheriff's Department (LASD): LASD operates the Incident Reporting Information System (IRIS), an information sharing data warehouse. IRIS leverages COPLINK software from Knowledge Computing Corporation (KCC). IRIS integrates information from LASD's records management, citation, jail information, and dispatch systems into a single database that allows quick search capability for crime analysis and investigative purposes.

DHS Information Queried:

Member agencies have the ability to query law enforcement records maintained in

(1) DHS/CBP-006 TECS,[4]

(2) DHS/ICE-011 Enforcement Integrated Database (ENFORCE), and[5]

(3) DHS/NPPD/USVISIT/PIA-002(b) Enumeration Services of the Automated Biometric Identification System (IDENT).[6]

Purposes for Information Sharing:

- Criminal Law Enforcement Purposes, which are defined as investigation of alleged violations of law where DHS or the member agencies have the authority to enforce or support the enforcement of the law.

---

[4] The PIA for DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing December 23, 2010, is located here: http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf. The SORN is DHS/CBP-011 last published December 19, 2008 (73 FR 77778)

[5] The PIA for DHS/ICE/PIA-015 Enforcement Integrated Database (EID) January 14, 2010, is located here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf. The SORN is DHS/ICE-011 published May 3, 2010 (75 FR 23274)

[6] DHS/NPPD/USVISIT/PIA-002(b) Enumeration Services of the Automated Biometric Identification System (IDENT), is located here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_enumeration.pdf. The SORN is DHS/USVISIT-0012 - DHS Automated Biometric Identification System (IDENT) published June 5, 2007 (72 FR 31080).

- National or homeland security purposes are those activities undertaken to identify, prevent, interdict, deter, or disrupt threats to the United States, its people, property, or interests, including threats involving terrorist activity, the use of weapons of mass destruction, and other threats and hazards to the nation where DHS or the member agency has such authority.
- Background checks purposes are only when conducting a background check on applicants seeking employment with the member agency.

How is the information accessed?

- Member Agencies query ICEPIC through the LEIS Service via their own internal IT application.

Do DHS ICEPIC users have query capabilities to new data based on the MOAs?

- Yes, DHS ICEPIC users are able to query the above member agencies' sensitive but unclassified law enforcement systems for the above mentioned purposes. To access the LEIS Service, ICEPIC has been modified to permit DHS ICEPIC users to query the LEIS Service and display results containing the above member agencies' law enforcement information from state and regional systems.

Is the information sharing covered by the ICEPIC SORN?

- Yes. The ICEPIC SORN covers this sharing.

I. Member Agencies with One-Way Query of DHS Information:

- International Justice and Public Safety Network (Nlets)

Information Shared:

Law Enforcement records maintained in

(1) DHS/CBP-006 TECS,[7]

(2) DHS/ICE-011 Enforcement Integrated Database (ENFORCE), and[8]

[7] The PIA for DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing December 23, 2010, is located here: http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf. The SORN is DHS/CBP-011 last published December 19, 2008 (73 FR 77778)

[8] The PIA for DHS/ICE/PIA-015 Enforcement Integrated Database (EID) January 14, 2010, is located here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf. The SORN is DHS/ICE-011 published May 3, 2010 (75 FR 23274)

(3) DHS/NPPD/USVISIT/PIA-002(b) Enumeration Services of the Automated Biometric Identification System (IDENT).[9]

The Purposes for Information Sharing are:

- Criminal Law Enforcement Purposes, which are defined as investigation of alleged violations of law where DHS or the member agencies have the authority to enforce or support the enforcement of the law.
- National or homeland security purposes are those activities undertaken to identify, prevent, interdict, deter, or disrupt threats to the United States, its people, property, or interests, including threats involving terrorist activity, the use of weapons of mass destruction, and other threats and hazards to the nation where DHS or the member agency has such authority.
- Background checks on applicants seeking employment with the member agency.

How is the information accessed?

- Information is accessed through system to system interface.

Do ICEPIC users have query capabilities to new data based on the MOAs?

- No.

Is the information sharing covered by the ICEPIC SORN?

- Yes. The ICEPIC SORN covers this sharing.

[9] DHS/NPPD/USVISIT/PIA-002(b) Enumeration Services of the Automated Biometric Identification System (IDENT), is located here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_enumeration.pdf. The SORN is DHS/USVISIT-0012 - DHS Automated Biometric Identification System (IDENT) published June 5, 2007 (72 FR 31080).