Privacy Impact Assessment
for the

Law Enforcement Information Sharing Service (LEIS Service)

DHS/ICE/PIA-051

June 28, 2019

Contact Point
Derek N. Benner
Acting Executive Associate Director,
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) owns and operates the Law Enforcement Information Sharing Service (LEIS Service or Service). The LEIS Service enables domestic law enforcement agencies outside of DHS to query certain information contained in DHS systems, and also permits authorized DHS law enforcement officials and analysts to query data from other law enforcement entities that have signed agreements with DHS to use the Service.[1] All entities querying the LEIS Service must have a signed agreement. The LEIS Service is a non-public facing web service that functions as a back-end super highway data sharing system. The LEIS Service was previously described in a Privacy Impact Assessment (PIA) update published in 2011 under the ICE Pattern Analysis and Information Collection (ICEPIC) system. In 2012, ICEPIC was replaced by the DHS Pattern and Information Collaboration Sharing System (DPICS2), which was subsequently retired in 2014. Since that time, the LEIS Service has been operating independently. ICE is issuing this PIA to discuss the privacy risks and mitigations with collecting, using, disseminating, and storing information related to the LEIS Service.[2] Once this PIA is issued, the previous PIA will be retired.

Overview

The LEIS Service facilitates sharing of information between DHS and external federal, state, local, tribal, and international law enforcement agency partners, or official organizations acting on behalf of those law enforcement agency partners (member agencies).[3] Member agencies must sign a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) stipulating that they will only use the LEIS Service for certain purposes.[4] There are three authorized purposes for using the LEIS Service to conduct a query: 1) criminal law enforcement; 2) national or homeland security purposes; 3) or to support applicant background checks conducted by the member agency. These uses are consistent with the source systems that the LEIS Service

[1] All of the member agencies involved are law enforcement agencies with the exception of Nlets, which is a state-owned non-profit that acts on behalf of law enforcement. They act in the same way as the rest of the member agencies and must abide by the terms of the Memorandum of Agreement. For the purposes of this PIA, Nlets will be included in any statement referring to "law enforcement agency partners" or "member agencies."

[2] DHS is retiring DHS/ICE/PIA-004 ICE Pattern Analysis and Information Collection (ICEPIC) with the publication of this PIA because ICEPIC and its successor DHS Pattern and Information Collaboration Sharing System (DPICS2) are now retired. The LEIS Service was originally described in the DHS/ICE/PIA-004(a) ICEPIC PIA Update, published on October 26, 2011. Because ICEPIC and DPICS2 were the systems that stored data shared by the LEIS Service, their retirement required ICE to have the LEIS Service pull records from the source systems directly, without the need for a records repository of copies. Other than this change, the operation of the LEIS Service is largely the same as was described in the October 2011 PIA Update referenced above. The PIAs can be found at www.dhs.gov/privacy.

[3] Most information sharing is two-way, however the LEIS Service is capable of only one-way information sharing, as explained in the Appendix to this PIA.

[4] All such agreements will be referred to in this document as Memoranda of Agreement (MOAs).

accesses.[5] 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, and alien smuggling.[6]

The member agencies (also referred to as parties herein) use the LEIS Service to access filtered DHS information for the purposes stated above. The LEIS Service, which does not have its own users or user interface, is strictly a back-end data sharing service that facilitates the exchange of data among member agencies. Each member agency uses its own user interface, referred herein as Information Sharing Service, to access the LEIS Service.[7]

Member agencies participate in their own respective federal, state, local, tribal, regional, or international Information Sharing Service to obtain limited sensitive but unclassified DHS criminal law enforcement information. Individuals within these organizations undergo background checks before they are authorized to access the LEIS Service, in accordance with the MOAs each member agency signs with DHS. The DHS data available through the LEIS Service uses the ICE PRIME Interface Hub (PRIME Interface Hub),[8] which transmits queries to and from U.S. Customs and Border Protection's (CBP) Modernized TECS, and ICE's Enforcement Integrated Database (EID).[9] Information pulled from EID also includes biometric information, limited to booking photographs, which is ultimately stored in Office of Biometric Identity Management (OBIM) systems.[10] When an individual is arrested by ICE, these booking photographs are enrolled in OBIM systems from EID.

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).[11] This section of the law authorizes the establishment and

---

[5] LEIS Service accesses information from three DHS systems of records: DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN, 81 FR 72080 (Oct. 19, 2016); DHS/CBP-011 TECS SORN, 73 FR 77778 (Dec. 19, 2008); and DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018), *available at* www.dhs.gov/privacy. For more information on the source systems, see Section 1.2 and the Appendix to this PIA. For more information on the authorities for using the LEIS Service, see Section 1.1 for the legal authorities underlying the LEIS Service.

[6] For a more comprehensive list of the types and subjects of information, see the Appendix to this document.

[7] Hereafter, references to Information Sharing Services will mean any information sharing service that has signed an MOA with DHS to participate in the LEIS Service. Examples of Information Sharing Services are the National Law Enforcement Telecommunications System (Nlets), the U.S. Department of Justice's National Data Exchange (NDEx), and the Texas Data Exchange (T-DEx). A complete list of Information Sharing Services can be found in the Appendix to this PIA.

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

[9] *See* DHS/CBP/PIA-021 TECS System: Platform and DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* www.dhs.gov/privacy.

[10] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

[11] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct*

operation of information sharing systems to enhance the investigation and prosecution abilities of participating law enforcement agencies. The terms of the MOAs are structured to permit member agencies access to information through their own Information Sharing Services.

The LEIS Service's primary purpose is to provide member agencies with access to DHS law enforcement data related to persons of interest, including suspects in child pornography, drug smuggling, immigration fraud, terrorism, alien smuggling, and in other instances in which 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 Sharing Services, law enforcement personnel at member agencies can query the LEIS Service to access certain information related to DHS criminal and national security investigations by basing their queries on information from the following categories: 1) *Name* (Full Name, First Name, Last Name, Middle Name, and Date of Birth); 2) *Identifying Number* (Social Security number, Passport number, Alien Number, encounter identifier, Driver License number); 3) *Address* (Full Address, Number, Street, Secondary Unit, City, State, Country, Postal Code, phone number); and 4) *Incidents* (Activity Number, activity description). Items included in the above parentheticals are the only information that can be queried. Multiple categories of information can be included; however, only one of each type of information within a category (e.g., one full name, one address) may be queried at a time. Biometrics, restricted to booking photographs, will also be provided in response to a query using the above identifiers. Booking photographs cannot be used to make queries.

Before the LEIS Service was 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. It improves the efficiency and automation of information sharing between DHS and its law enforcement partners beyond what previously existed using manual email and telephone-based information sharing.

What DHS Information is Shared with Member Agencies Through the LEIS Service?

Only a limited subset of DHS information is made available to member agencies through the LEIS Service. The Appendix to this PIA provides greater detail on which information is shared according to the information sharing MOAs and will be updated if and when new MOAs are signed, to provide greater transparency.

How DHS Information is Shared with Member Agencies through the LEIS Service?

Only member agencies that have entered into MOAs with DHS are provided computer connectivity to the LEIS Service. To access the LEIS Service, the connecting Information Sharing

---

Terrorism Act (USA PATRIOT Act) (Oct. 26, 2001), as amended, Pub. L. No. 107-56, 34 U.S. C. § 10321(b)(4).

Services are modified to permit member agencies authorized users (law enforcement personnel) to query the LEIS Service and display results containing select DHS law enforcement information. DHS relies upon the member agencies to vet and authenticate appropriate users of the LEIS Service. DHS also relies on the member agencies to make appropriate use of the LEIS Service in accordance with the MOA with DHS. Importantly, the LEIS Service MOAs prohibits member agencies from storing DHS information on their computers, storage media, and from printing the data. The system is designed so that information accessed through the LEIS Service is displayed on the user's screen but does not generate a document that can be saved or stored. However, since users access LEIS Service information through an intermediary information sharing service, there is no technical way for the LEIS Service to prevent screenshots or printing of accessed information.

To conduct a query using the LEIS Service, the user inputs a search query into his or her Information Sharing Service interface connected to the LEIS Service. The search query is transmitted to the LEIS Service in search of a matching name or identifying number records contained in the DHS source systems listed in this PIA. Records are pulled from these databases through the PRIME Interface Hub. If matching records are found, the LEIS Service then extracts the data fields permitted for sharing through the LEIS Service and displays it to the authorized member agency user. The member agency user never "logs in" to the LEIS Service, but rather queries the Service and receives the response through its own Information Sharing Service interface.

Member agencies may only conduct single queries based on a single individual's identifiers; the LEIS Service does not allow 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 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. The results also provide the member agency with instructions to contact DHS via the Law Enforcement Support Center, as needed, for purposes of case deconfliction and information sharing to support the law enforcement interests of DHS and the member agencies.

How Member Agencies Use Information Shared Through 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 investigation of alleged violations of criminal law in which 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, pursuant to the terms of the MOAs, member agencies cannot release any information obtained through the LEIS Service to third parties 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' Law Enforcement Data

The LEIS Service allows for sharing of data between DHS and the member agencies' Information Sharing Services.[12] DHS users are able to access member agencies' law enforcement data entered into an Information Sharing Service, consistent with Section 701 of the USA PATRIOT Act.[13] The technical means by which DHS users may access this data is an interface between the LEIS Service and the Analytical Framework for Intelligence (AFI) system, which is owned by U.S. Customs and Border Protection (CBP).[14] DHS users log into AFI and have the option to query data maintained in the Information Sharing Services, using the LEIS Service as the back-end interface.[15] DHS users may view, but not store, member agency law enforcement data in this manner using the LEIS Service through AFI. This data exchange between DHS and member agencies has been implemented as a National Information Exchange Model (NIEM)-compliant Law Enforcement Information Sharing Program (LEISP) Logical Entity eXchange Specifications (LEXS) 2.0/3.1 data exchange interface.[16]

Accountability, Security, and User Auditing

Before a member agency is granted access to the LEIS Service, it must certify to DHS that its users have undergone background checks that require, at a minimum, criminal history and national fingerprint checks. In addition, the Information Sharing Services and the LEIS Service have audit capabilities. The LEIS Service logs the date, time, subject, and originating account of all user queries. These audit logs are maintained until business use ceases. The results of the audit reports or other internal investigations related to performance under the MOAs are shared between the parties upon request.

---

[12] For a list of information sharing services with two-way sharing and one-way sharing agreements see the Appendix to this document.
[13] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA PATRIOT Act) (Oct. 26, 2001), as amended, Pub. L. No. 107-56, 34 U.S. C. § 10321(b)(4).
[14] *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) PIA, *available at* www.dhs.gov/privacy.
[15] The LEIS Service is strictly a back-end data sharing service that facilitates the exchange of data among participating systems. The Service does not have users or a user interface. Users must log in to a participating system, like AFI or one of the Information Sharing Services, to perform a query that uses LEIS.
[16] LEXS defines a common format in which information can be shared. It specifies how law enforcement information should be packaged and delivered to information sharing applications and how partnering applications can implement federated search capabilities.

Information provided through the LEIS Service is encrypted during delivery between the DHS Network and the Information Sharing Service. In addition, the LEIS Service validates the registered security certificates of the Information Sharing Services to verify the identity of the member agency user prior to sending any information. The LEIS Service records every incoming and outgoing message. Originating Agency Identifiers, user identification numbers, and other metadata are collected for every transaction. These audit logs are maintained in a database until business use ceases. The results of the audit reports or other internal investigations related to performance under the MOAs are shared between the parties upon request.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

ICE has been authorized to collect information under Section 701 of the USA PATRIOT Act;[17] 6 U.S.C. § 112; 8 U.S.C. §§ 1105, 1103(a)(4), 1357(a); and Executive Order 13388.[18] Pursuant to the Homeland Security Act of 2002,[19] the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include laws residing in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this enforcement authority to the Director of ICE in DHS Delegation Number 7030.2, *Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the Department of Homeland Security* (January 30, 2003).[20]

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The LEIS Service was formerly connected to and a part of the ICEPIC IT environment, and was covered by the DHS/ICE-002 ICEPIC System of Records Notice (SORN).[21] Due to the retirement of ICEPIC and its successor system known as DPICS2, ICE will be retiring the DHS/ICE-002 ICEPIC SORN once the source system SORNs listed below are updated to include a new routine use that will address sharing through the LEIS Service. The LEIS Service will be covered by the source system SORNs below from which the LEIS Service pulls data.

---

[17] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (USA PATRIOT Act) (Oct. 26, 2001), as amended, Pub. L. No. 107-56, 34 U.S.C. § 10321(b)(4).
[18] Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," 70 FR 62023 (Oct. 27, 2005).
[19] Pub. Law 107-296, 6 U.S.C. §§ 101-629.
[20] *See* DHS Delegation Number 7030.2, *Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the Department of Homeland Security* (January 30, 2003), *available at* https://www.hsdl.org/?abstract&did=234774.
[21] *See* DHS/ICE-002 ICE Pattern and Analysis and Information Collection (ICEPIC), 73 FR 48226 (Aug. 18, 2008).

- DHS/CBP-011 TECS SORN[22] (CBP and ICE Subject Records only);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN;[23] and
- DHS/ALL-041 External Biometric Records (EBR) SORN.[24]
- The forthcoming DHS-wide Enterprise Biometric Administrative Records (EBAR) SORN.

For more information about these SORNs and external sharing of data from the LEIS Service, see Section 6 and the Appendix to this PIA.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The LEIS Service falls within the security boundary for another system known as HSI Data Warehouse. HSI received its authority to operate (ATO) on May 18, 2016 and will expire on May 12, 2019.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No. LEIS Service produces an audit log that tracks query related information such as date, time, and subject of query, user ID of the individual running the query, information the query was searching, and what DHS information is disclosed and to whom. This log is retained until business use ceases, then destroyed. No other records are maintained by the LEIS System.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

ICE does not collect personally identifiable information (PII) directly from individuals or enterprises for inclusion in the LEIS Service. The DHS data shared through the LEIS Service with external law enforcement partners is not subject to the Paperwork Reduction Act. The information

[22] *See* DHS/CBP-011 TECS SORN, 73 FR 77778 (Dec. 19, 2008). *See* DHS/CBP/PIA-021 TECS System: Platform and DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* www.dhs.gov/privacy.
[23] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN, 81 FR 72080 (Oct. 19, 2016). There have been multiple PIA updates published for the associated IT system from which these records are obtained, the Enforcement Integrated Database. *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* www.dhs.gov/privacy.
[24] DHS/ALL-041 External Biometric Records (EBR) System of Records, 83 FR 17829 (April 24, 2018).

collected through the LEIS Service may have been originally collected by other government agencies using forms that are subject to the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The LEIS Service is supported by ICE and CBP databases containing DHS records that are available through the PRIME Interface Hub for search by external Information Sharing Services.[25] Queries must contain person information, location information, a number associated with an incident, or an identifier (only one data element from each category may be included in a query). In the event of a match, the LEIS Service retrieves a set of predetermined filtered data fields from the matching records and delivers them to users through their respective Information Sharing Service. The LEIS Service also facilitates the same query/response capability in the opposite direction, specifically the delivery of queries made by DHS users via the CBP's AFI, with responses received from Information Sharing Services for any matching records.

The DHS data shared through the LEIS Service is structured data consisting of filtered data fields from DHS law enforcement records permitted to be shared outside of DHS without violating laws or policies, or interfering with ongoing DHS investigations. DHS law enforcement records relate to persons of interest, including suspects in child pornography, drug smuggling, immigration fraud, alien smuggling, and a wide range of other cases. Information available to member agencies is discussed in the Appendix. Query responses are delivered through the same interface used to query the LEIS Service (i.e., for DHS personnel, AFI; for member agency personnel, the relevant Information Sharing Service). The technology does not allow the response data to be downloaded or retained, only displayed.

2.2 What are the sources of the information and how is the information collected for the project?

DHS law enforcement data is obtained via electronic feed or transfer from two DHS law enforcement IT systems: ICE's Enforcement Integrated Database (EID)[26] and CBP's TECS System.[27] As noted above, some of the biometric information shared through the LEIS Service is ultimately stored in OBIM systems, but the information is pulled from EID and TECS.

---

[25] *See* DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), *available at* www.dhs.gov/privacy.
[26] There have been multiple PIA updates published for the Enforcement Integrated Database. *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* www.dhs.gov/privacy.
[27] *See* DHS/CBP/PIA-021 TECS System: Platform and DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* www.dhs.gov/privacy.

Member agencies obtain the information they submit in the form of queries to the LEIS Service during investigations or other law enforcement activities using traditional investigative techniques.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. All data transmitted through the LEIS Service is obtained from government law enforcement records.

2.4 Discuss how accuracy of the data is ensured.

The MOAs require the parties to make reasonable efforts to ensure the accuracy of the data shared through the LEIS Service. The parties further agree to inform each other if they receive a challenge to, or question about, the accuracy of any data obtained through the Service.

The use of data by member agencies may not be used as a basis for a law enforcement action (e.g., cannot use information as the sole basis for an arrest warrant) or disseminated for any other purpose, or in any other manner outside the member agency, unless the member agency obtains the express permission of the DHS Component that owns the underlying information. Not only does this provide DHS the opportunity to check records for accuracy before the records are relied upon to support a law enforcement action, but it also helps ensure that the member agency fully understands the context of the information provided.

The MOAs generally require member agencies to annotate the source of information as the LEIS Service and the date the information was obtained in internal documentation. This helps to ensure traceability of the data back to DHS as the owner and source for purposes of verification. This also helps to ensure that any person reviewing the information at a later time has a sense of the age of the data.

The member agencies are responsible for ensuring the accuracy of information accessible through the LEIS Service. Since the data is used to support criminal investigations, national and homeland security, as well as background checks, law enforcement personnel who access DHS's data through the LEIS Service will compare the information against other data systems and sources, increasing the likelihood that inaccurate or inconsistent data is discovered. These checks are likely to occur before any law enforcement decisions are made, such as a decision to charge an individual with a crime. In the case of background checks, an individual will typically have a right to obtain a copy of the background check data upon which the agency relied, and may challenge its accuracy. The same is true for criminal investigations, and for some homeland security actions, in which the individual is afforded an opportunity to access, review, and challenge the accuracy of

data relied upon to make an adverse determination (e.g., criminal charges, or denial of a license on homeland security grounds).

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the law enforcement data collected and shared via the LEIS Service is inconsistent with the purposes for which it was collected, or is overly broad to accomplish the purpose of the Service.

Mitigation: The data collected and shared through the LEIS Service is intended to support law enforcement information sharing among DHS and other federal, state, local, tribal, and international law enforcement partners. The DHS data shared is appropriately limited to law enforcement data only, and originates from DHS law enforcement components of ICE and CBP. ICE and CBP collected this information in the course of their law enforcement missions in the areas of border security, criminal law enforcement, criminal investigations, and immigration enforcement. The data use restrictions imposed on the member agencies, all of whom are law enforcement agencies, ensure that the use of this information is consistent with the original law enforcement purposes for which DHS originally collected the data. The MOAs provide that information exchanged through the LEIS Service with member agencies may only 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 terms of the MOAs, DHS information accessed by member agencies through the LEIS Service may not be accessed, or used for any other purpose, including general licensing and eligibility for federal or state benefits.

Privacy Risk: Since individuals have generally not participated in the collection of their information that is shared through the LEIS Service, there is a risk that such information may not be accurate or complete.

Mitigation: This risk is partially mitigated. Individual participation in the collection of data is typically very limited in a law enforcement context. By their nature, criminal and other types of investigations must often operate covertly to gather evidence sufficient to meet the requisite burden of proof and to demonstrate culpability in court. For instance, opportunities for targets of criminal investigations may not to be aware that their personal information is being collected. Additionally, the accuracy of information provided by a suspect may be questionable if the individual is seeking to avoid being caught engaging in illegal behavior. In the event that data obtained through the LEIS Service is used to support an adverse decision about an individual (e.g., charge the individual with a crime), then he or she will typically have a right to access and review that data. The individual will have the opportunity through criminal, civil, or administrative

proceedings to challenge the accuracy of that information. These due process protections partially mitigate the risk stated above.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The LEIS Service facilitates the sharing of information among participating law enforcement agencies about subjects of law enforcement interest. Identifiers such as name, alias, date of birth, Federal Bureau of Investigation (FBI) Universal Control Number (UCN), Social Security number (SSN), may be shared, as well as limited information about the type of DHS law enforcement investigation or encounter (e.g., immigration arrest, target of a border seizure). This information is used to help the query/response feature of the LEIS Service function properly, but is also used to accomplish the purpose of the LEIS Service, which is to enhance information sharing among law enforcement agencies for law enforcement purposes.[28]

Only member agencies that have signed an LEIS Service MOA are allowed to connect to the LEIS Service. These agreements spell out the terms and conditions for accessing the LEIS Service and the authorizations and limitations for use, disclosure, retention, safeguarding, and destruction of information accessed through the LEIS Service. For instance, generally, MOAs state that LEIS Service information may not be accessed or used for any other purpose, including general licensing, employment, and eligibility for federal or state benefits, and background investigations not related to employment with the member agency.

The member agencies are prohibited from any onward transfer of data received through a LEIS Service beyond the member agency personnel who have direct access to the LEIS Service, and there may not be any retention of the data, unless express permission is obtained from DHS.

The information provided through the LEIS Service remains in the custody and control of DHS and is subject to release only in accordance with federal law, including the Freedom of Information Act[29] and the Privacy Act of 1974.[30] The member agencies are generally required to notify DHS upon becoming aware of a lawsuit or proceeding that seeks access to the LEIS Service information.

The Appendix provides additional details on the information sharing and will be updated periodically as new MOAs are signed.

[28] The entire list of data elements shared through the LEIS Service is information that is not publicly disclosed to preserve the integrity and effectiveness of this law enforcement tool.
[29] 5 U.S.C. § 552.
[30] 5 U.S.C. § 552a.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. The LEIS Service does not have a user interface. It relies on other systems, such as AFI and the member agencies' Information Sharing Services, to provide an interface for users. The LEIS Service provides and regulates the back-end exchange of data between the parties' systems and data repositories in compliance with the MOAs.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that authorized users will access information through the LEIS Service for unauthorized purposes.

Mitigation: This risk is partially mitigated. Before DHS grants access to the LEIS Service, a member agency must first certify to DHS that their users have undergone background checks that require, at a minimum, criminal history and national fingerprint checks. This helps to ensure the suitability of those who are given access to sensitive law enforcement data. The MOAs also require auditing of users through logging their activities querying the LEIS Service, as a way to discourage and detect inappropriate user behavior, so appropriate disciplinary action can then be taken. The MOAs require that the Information Sharing Services log the date, time, subject, and originating account of all user queries, and that logs be maintained until business use ceases. The parties must also cooperate with reasonable requests for information from each other as necessary to allow oversight to ensure the proper execution and implementation of the terms of the MOAs. Finally, the parties are obligated to share the results of audit reports or other internal investigations related to their performance under the MOAs. These provisions provide a mechanism for user misconduct to be detected, and accountability for the law enforcement agencies that employ the user if they do not properly investigate and respond to instances of inappropriate use.

Privacy Risk: There is a risk that unauthorized persons will access sensitive information being shared through the LEIS Service by exploiting security vulnerabilities.

Mitigation: Information shared through the LEIS Service is encrypted during delivery between the DHS Network to the Information Sharing Services. In addition, the LEIS Service validates the registered security certificate of the Information Sharing Services and member agencies' systems to verify the identity of the member agency user prior to sending any

information to the user. Security controls for the LEIS Service are monitored by the ICE Security Operations Center and the Information System Security Officer (ISSO) for the LEIS Service. The system is subject to an on-going authorization at DHS, which provides continuous security monitoring of the environment to detect anomalies and indications of breach or compromise of the data or system. Additionally, the partners who sign LEIS Service MOAs expressly agree to notify DHS immediately in the event a loss or compromise of the data is suspected in their environment. Although these security controls mitigate the risk that a security event will occur or remain undetected, there is no guarantee that this system is immune to compromise due to continuously evolving security threats.

Privacy Risk: There is a risk that information will be retained, despite the LEIS Service offering no functionality to do so.

Mitigation: This risk is not mitigated, however the risk is low that information will be improperly retained. Since users access the LEIS Service through an intermediary Information Sharing Service, there is no technical way for the LEIS Service to prevent screenshots of accessed information. However, the MOAs signed by the member agencies prohibit the retention of data by any authorized users without additional express permission from DHS to retain the information. Further, the LEIS Service does not send original records or copies of records in response to queries. The user receives a screen with information filling fields on the screen. There is no built-in functionality allowing for printing or saving information.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

General notice of the existence, contents, and uses of LEIS Service is provided by the publication of this PIA and the SORNs for the underlying DHS data delivered by the LEIS Service. Any notice of collection is covered by the privacy documentation for the source systems. Because this system is used for a law enforcement purpose and contains sensitive information related to criminal and civil investigations, it is not feasible or advisable to provide notice to individuals at the time their information is accessed by the system. When law enforcement agents and officers interact with individuals in connection with an investigation, however, the subjects are generally aware that their information will be recorded and stored. Furthermore, information is frequently collected through other lawful means, such as by subpoenas and search warrants. If information is obtained from individuals through Federal Government-approved forms or other means, such as information collected pursuant to seizures of property, or notices on forms that state information may be shared with law enforcement entities.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The LEIS Service does not collect information directly from individuals. The information is collected by other systems. In most cases, because of the DHS law enforcement, immigration, or intelligence purposes for which the information is collected, opportunities to refuse consent may be limited or nonexistent.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: A risk exists that the public is not aware of the LEIS Service, or that individuals may not be aware that DHS is sharing their information with law enforcement partners.

Mitigation: The ICEPIC PIA, which originally described the LEIS Service, was published by DHS in 2011, and provided significant public transparency to the operation, purpose, use and privacy protections of this information sharing service.[31] Although this PIA will replace the 2011 ICEPIC PIA, DHS continues to provide the same level of transparency and sufficient information to allow the public to pursue requests to access or amend their data, when permissible. This PIA also lists the law enforcement partners with which DHS shares information using the Service.

Privacy Risk: There is a risk that information shared by DHS through the LEIS Service is incorrect and could prejudice the individual, but the individual is unaware of the existence of the data, how to access it, or the means to correct it.

Mitigation: This risk is partially mitigated. In the context of an ongoing law enforcement mission, providing a suspected violator with notice or the opportunity to consent to the use of his or her information will compromise the ability of law enforcement agencies to effectively enforce the law, and could put law enforcement officers at risk. For this reason, notice of collection and the opportunity to consent to specific uses of the data available through systems like the LEIS Service are generally not provided. Moreover, no records are stored within the LEIS Service. All records are drawn from the source systems. For more information regarding exemptions from disclosure or amendment, see the source system SORNs.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

LEIS Service queries performed by external partners using an Information Sharing Service are retained by ICE in an audit log until business use ceases. DHS responses to these queries are

[31] *See* DHS/ICE/PIA-004(a) ICE Pattern Analysis and Information Collection System (ICEPIC), *available at* www.dhs.gov/privacy.

not retained by the querying user beyond a specific query session. Although a user might be able to print a screen shot of the LEIS response, this violates the terms of the signed MOAs.

LEIS Service queries performed by DHS personnel using the AFI interface should only be retained by the relevant member agencies' Information Sharing Service in an audit log until the business use ceases. Responses to queries of Information Sharing Services through the LEIS Service are not retained by the LEIS Service. The LEIS Service records every incoming and outgoing message, including both queries and responses. The stored queries and responses can only be searched by the metadata collected for each transaction (e.g., user identification numbers, time, type of message, originating agency identifiers). The content of the queries and responses in the LEIS Service cannot be searched (e.g. a user cannot search the stored queries and responses using a name, address, or date of birth or other data). These audit logs are maintained in a database until its business use ceases.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the operation of the LEIS Service results in PII pulled from source systems being retained for longer than the retention period for the source systems themselves.

Mitigation: The LEIS Service was designed so that it does not maintain DHS or member agency records that are queried. The LEIS Service only maintains audit logs on the queries to the Service—and not DHS's responses to those queries—until the business use ceases. The same is true for the Information Sharing Services used by the member agencies. Additionally, the Service does not provide member agencies or DHS users with the functionality to download or retain responsive information. This design promotes the Fair Information Practice Principles of data minimization (i.e., retain information for a minimum amount of time necessary to accomplish a mission) and audit and accountability (i.e., ensure compliance with the actual use of the information).

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. The primary purpose of the LEIS Service is to facilitate the two-way exchange of law enforcement data between DHS data and external law enforcement agencies that use Information Sharing Services. The specific agencies and Information Sharing Services that are engaged with the LEIS Service are listed in the Appendix, which will be updated as this information changes. Each external law enforcement agency grants its personnel access to an Information Sharing

Service that is covered by an MOA with DHS. These users log into their own respective Information Sharing Service, which connects to the LEIS Service, and query DHS data in the LEIS Service source systems. The response is then transmitted from DHS to the Information Sharing Service, and viewed by the authorized user who submitted the query.

Only federal, state, local, tribal, regional, or international member agencies that have entered into the LEIS Service MOAs are provided connectivity to the LEIS Service. These agreements spell out 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. The MOAs govern the authorized uses of the data queried through LEIS Service, the level of information security of the systems querying DHS through the LEIS Service, and the authentication of users. 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 PII contained in the DHS law enforcement records.

Authorized uses of the data are limited to 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 through the LEIS Service may not be accessed or used for any other purpose.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The primary purpose of the LEIS Service is to provide member agencies with access to DHS law enforcement data related to persons of interest, including suspects in child pornography, drug smuggling, immigration fraud, alien smuggling, and in other instances in which a member agency has a predicated reason to identify such persons of interest for a criminal law enforcement purpose. The sharing of PII with law enforcement agencies outside of DHS is compatible with the law enforcement purposes for the original collection of information, listed in the four SORNs applicable to the underlying data sources. For more information about the source SORNs for this service, see the Appendix to this document.

In coordination with the publication of this PIA, ICE will update the relevant SORNs with a specific routine use that describes sharing information with LEAs through LEISS. After this routine use is added to the SORNs, the ICEPIC SORN will be retired with a notice of rescindment published in the Federal Register.

6.3 Does the project place limitations on re-dissemination?

Yes. Specific provisions in the LEIS Service MOAs require that the data obtained through the LEIS Service may not be further transferred beyond the member agency personnel who have direct access to the LEIS Service. Federal agencies that receive LEIS Service information are

subject to the Privacy Act and, as such, may not re-disclose information covered by that law without clear authority to do so under their applicable SORNs. Under the terms of the MOAs, information obtained by all member agencies through the LEIS Service cannot be further disclosed by the member agency without obtaining prior written consent from DHS.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The LEIS Service has an audit log that tracks the queries of DHS information, DHS information that is disclosed, and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: A risk exists that personal information could be inappropriately shared with outside agencies that do not have an MOA, contrary to the stated purpose and use of the original collection.

Mitigation: This risk is partially mitigated. The LEIS Service requires any Information Sharing Service to sign an MOA outlining the limits of use for any information accessed through the service. Specific provisions in the LEIS Service MOAs require that data obtained through the LEIS Service may not be further transferred beyond the member agency personnel who have direct access to the data through the LEIS Service. Finally, the LEIS Service does not provide copies of records that can be saved and further disseminated. Therefore, there is no way for an LEIS Service user to directly share information with an outside party using the LEIS Service.

Privacy Risk: There is a risk that member agencies may use the limited information provided by the LEIS Service as the sole determining factor in making a decision on a law enforcement matter. This could potentially lead to mismanagement of law enforcement investigations.

Mitigation: The LEIS Service MOAs require that the information provided to member agency be used only to open up avenues of an investigation. That information may not be relied upon as the sole determining factor in any decision making in a law enforcement matter. For example, a member agency that obtained information from the LEIS Service could not use that information as the sole basis for an arrest warrant.

Privacy Risk: There is a risk that information provided by the LEIS Service to member agencies could be accessed by or improperly shared with unauthorized individuals.

Mitigation: This risk is partially mitigated. Specific provisions in the LEIS Service MOAs require that data obtained through the LEIS Service may not be further transferred beyond the member agency personnel who have direct access to the data through the LEIS Service. Also, the LEIS Service keeps an audit log that logs the date, time, subject, and originating account of all

user queries to the LEIS Service in order to monitor which users access information. This audit log is reviewed weekly to ensure that the LEIS Service is not being used improperly. Finally, the LEIS Service does not provide copies of records that can be saved and further disseminated.

Section 7.0 Redress

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

The LEIS Service does not maintain any subject records. However, individuals subject to the Privacy Act (U.S. Citizens, Lawful Permanent Residents, and those covered by the Judicial Redress Act[32]) may request access to records about themselves in source systems by following the procedures outlined in the SORNs that cover the DHS records available through the LEIS Service. Those SORNs are listed in the response to Question 1.2. Individuals not covered by the Privacy Act can access their records through the Freedom of Information Act (FOIA). All or some of the requested information may be exempt from access under the Privacy Act and/or FOIA to prevent harming various types of agency interests, including law enforcement investigations or interests. Providing individual access to records contained in the LEIS Service could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit an individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

In addition to the procedures above, individuals seeking access to any record accessible from the CARIER system of records may submit a request to the ICE FOIA Office by mail or facsimile to the following address:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

Individuals seeking access to any record accessible from the TECS system of records may submit a request to the CBP FOIA Office by mail or facsimile to the following address:

FOIA Officer
U.S. Customs and Border Protection
90 K Street, NW

[32] *See* 82 FR 7860, Judicial Redress Act of 2015; Attorney General Designations for an explanation of the Judicial Redress Act and the countries covered by the Judicial Redress Act.

9th Floor, Mail Stop 1181
Washington, DC 20229

Individuals seeking access to any record accessible from OBIM biometric systems of records may submit a request to the Office of Biometric Identity Management (OBIM) Privacy Office by mail or facsimile to the following address:

Office of Biometric Identity Management Privacy
245 Murray Lane SW
Washington, D.C. 20598-0628
OBIMPrivacy@ice.dhs.gov

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The LEIS Service does not maintain any subject records. However, individuals covered by the Privacy Act (U.S. Citizens, Lawful Permanent Residents, and those covered by the Judicial Redress Act of 2015) seeking to correct records contained in the CARIER system of records, or seeking to contest its content, may submit a request by mail to:

U.S. Immigration and Customs Enforcement
Office of Information Governance & Privacy
Privacy Office
500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
(202) 732-3300
http://www.ice.gov/management-administration/privacy

Individuals covered by the Privacy Act (U.S. Citizens, Lawful Permanent Residents, and those covered by the Judicial Redress Act of 2015) seeking to correct records contained in the TECS system of records, or seeking to contest its content, may submit a request by mail to:

FOIA Officer
U.S. Customs and Border Protection
90 K Street, NW
9th Floor, Mail Stop 1181
Washington, DC 20229

7.3 How does the project notify individuals about the procedures for correcting their information?

ICE provides general notice on its public-facing website about the procedures for submitting FOIA and Privacy Act requests. The LEIS Service itself does not maintain any records aside from an audit log. However, each of the LEIS Service source SORNs for information

transmitted through the LEIS Service contains information about procedures for correcting records held in each source system. See question 1.2 for a list of the source SORNs for the LEIS Service.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to participate meaningfully in the use of their data as maintained in this system, or determine whether the system maintains records about them.

Mitigation: This risk is partially mitigated. The LEIS Service is used for law enforcement purposes, and as such, an individual's rights to be notified of the existence or non-existence of data about them, and how that data may be used by DHS, is limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools, such as wiretaps or surveillance, will no longer be useful. Permitting individuals to direct the agency's use of their information will similarly interfere with the intended law enforcement use of the system. Nevertheless, the publication of this PIA and the applicable SORNs provides general notice about DHS's collection and use of the information. Additionally, ICE has exempted investigative systems from access and amendment under the Privacy Act, though ICE will apply exemptions on a case-by-case basis at the time of the access or amendment request. In appropriate circumstances, therefore, individuals may have an opportunity to access or correct their records, consistent with law enforcement necessity.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The LEIS Service has audit capabilities that log the date, time, subject, and originating account of all user queries. The LEIS Service records every incoming and outgoing message, this includes both queries and responses. The stored queries and responses can only be searched by the metadata collected for each transaction (e.g., user identification numbers, time, type of message, originating agency identifiers). The content of the queries and responses in LEIS Service cannot be searched (e.g., a user cannot search the stored queries and responses using a name, address, or date of birth or other data). These audit logs are maintained in a database until its business use ceases

Audit logs are reviewed weekly by System Administrators or the ICE Security Operations Center. Any unusual events are disclosed to the ISSO. Any violation or criminal activity is reported to the Office of the Information System Security Manager (OISSM) team in accordance with the

DHS security standards, as well as ICE's Office of Professional Responsibility. If the auditing system is ever inactive, the LEIS Service cannot service any transactions until it is fixed.

The MOAs require that all information obtained through the LEIS Service be used only for official criminal law enforcement purposes, national or homeland security purposes, or to facilitate background checks for applicants seeking employment with the member organization.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

The MOAs signed by member organizations stipulate that information obtained from the LEIS Service must be handled in accordance with the Privacy Act of 1974 and other relevant laws and policies. Privacy training is the responsibility of the user's agency. LEIS Service does not provide any specialized privacy training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

According to the MOAs, before access to the LEIS Service is granted, users must demonstrate a need to access LEIS Service information in order to perform their respective job responsibilities. This is decided at the discretion of the member agency pursuant to its law enforcement mission.

Before a member agency is granted access to the LEIS Service, it must certify to DHS that its users have undergone background checks that require, at a minimum, criminal history, and national fingerprint checks. In addition, both the Information Sharing Services and the LEIS Service have audit capabilities. The LEIS Service logs the date, time, subject, and originating account of all user queries. These audit logs are maintained until its business use ceases. The results of the audit reports or other internal investigations related to performance under the MOAs are shared between the parties upon request.

Information provided through the LEIS Service is encrypted during delivery between the DHS Network and the Information Sharing Service. In addition, the LEIS Service validates the registered security certificates of the Information Sharing Services to verify the identity of the member agency user prior to sending any information

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All new information sharing agreements, to the extent they are required, will be reviewed by the program's information security officer, the ICE Privacy Officer, Office of the Principal Legal Advisor, key program stakeholders, and the program manager, and then sent to DHS for formal review. ICE MOAs articulate who will be using the shared information and how it will be used. If the terms of existing MOAs are changed, addenda will be established and reviewed by the appropriate parties before sending to DHS for formal review, to be approved as amendments to existing agreements.

Responsible Officials

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

Approval Signature

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

_____

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

Appendix

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

I. Law Enforcement Organizations with Two-Way Query Capability:

- 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.
- 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:

Information shared is limited to certain DHS records. These records are accessed from the following IT systems:

- CBP TECS (CBP and ICE Subject Records only); [33]
- ICE Enforcement Integrated Database (EID);[34] and
- The Office of Biometric Identity Management's (OBIM) biometric systems of records.

External agency users can only conduct single queries; the LEIS Service does not allow users to conduct batch queries or queries of multiple distinct names and/or distinct identifying numbers at one time.

All member agencies have access to the same data elements when querying the LEIS Service using their respective law enforcement systems. Only person subject records are shared from TECS and EID. Data from both TECS and EID systems is available for searching and receiving matching records contained in those systems. No unstructured text is shared through the LEIS Service.

ICE and CBP criminal case information available through the LEIS Service is limited to closed TECS subject records and certain ICE records from EID. TECS "subject records" is a generic term that includes enforcement or inspection records located in TECS pertaining to individuals. Subject records encompass not only violations of laws enforced by ICE and CBP, but may also include information on violations of other federal and state laws. Information contained in subject records, and available through the LEIS Service, includes 1) *Name* (Full Name, First Name, Last Name, Middle Name, and Date of Birth); 2) *Identifying Number* (Social Security number, Passport number, Alien Number, and an encounter identifier); 3) *Address* (Full Address,

[33] *See* DHS/CBP-011 TECS SORN, 73 FR 77778 (Dec. 19, 2008). *See* DHS/CBP/PIA-021 TECS System: Platform and DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* www.dhs.gov/privacy.

[34] *See* DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) SORN, 81 FR 72080 (Oct. 19, 2016). There have been multiple PIA updates published for the associated IT system from which these records are obtained, the Enforcement Integrated Database. *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* www.dhs.gov/privacy.

Number, Street, Secondary Unit, City, State, Country, Postal Code); 4) *Incident* (Activity Number, activity description); and 5) Biometrics (booking photographs).

Only TECS Person Subjects annotated as a "suspect" (not victim or witness) are shared. Information restricted by statute, regulation, or policy is filtered and not shared with member agencies. Examples of this type of information include:

- Bank Secrecy Act Information;
- Trade Secrets Act Information;
- National Security Information;
- Third Agency Information;
- Confidential Sources; and
- Undercover Operations.

Purposes for Information Sharing:

- Criminal Law Enforcement Purposes, which are defined as investigations of alleged violations of law in which 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 when DHS or the member agency has such authority; and
- When conducting a background check on applicants seeking employment with the member agency.

How is the information accessed?

Information is accessed through a system-to-system interface. The LEIS Service uses the PRIME Interface Hub, a back-end tool, to transmit user queries to various DHS systems. Information that is queried using the PRIME Interface Hub is then returned through the LEIS Service and displayed through the member agency's user interface. While the PRIME Interface Hub has the ability to query a wide variety of DHS systems, use through the LEIS Service will be limited to those listed above.

How long is the information retained?

The DHS records that are made available for query through the LEIS Service are not retained. DHS records are pulled by the LEIS Service through the PRIME Interface Hub from source systems and displayed through the member agency's user interface.

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

Yes, DHS personnel can query data through the LEIS Service through the CBP-owned Analytical Framework for Intelligence (AFI) system.[35] The AFI system connects to the LEIS Service to facilitate the sending of queries from DHS AFI users to the member agencies that have signed MOA's with DHS. The same purpose restrictions described above apply to these queries.

II. Law Enforcement Organization or Organization Working on Behalf of Law Enforcement with One-Way Query of DHS Information[36]:

- International Justice and Public Safety Network (Nlets)

DHS Information Shared:

Information shared is limited to certain DHS records. These records are accessed from the following systems of records:

- DHS/CBP-011 TECS SORN;
- DHS/ICE-011 CARIER SORN; and
- DHS/ALL-041 EBR SORN.

Member agency users can only conduct single queries; 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.

All member agencies have access to the same data elements when querying the LEIS Service using their respective law enforcement systems. Only person subject records are shared from TECS. Only person subject information is shared through the Enforcement Integrated Database (EID). Data from both TECS and EID systems are available for searching and receiving matching records contained in those systems. No unstructured text is shared through the LEIS Service.

ICE and CBP information available through the LEIS Service is limited to closed TECS subject records and certain ICE case records from EID. TECS "subject record" is a generic term

[35] *See* DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) PIA, *available at* www.dhs.gov/privacy.
[36] Please note that ICE is currently piloting a capability that permits ICE agents to query Canada through OBIM biometric systems using the Nlets portal on the LEISS network; since ICE will be able to send a query and receive a response, this pilot is considered a two-way service.

that includes the enforcement or inspection records located in TECS pertaining to individuals. Subject records encompass not only violations of laws enforced by ICE and CBP, but may also include information on violations of other federal and state laws. Information contained in subject records, and available through the LEIS Service, include 1) *Name* (Full Name, First Name, Last Name, Middle Name, and Date of Birth); 2) *Identifying Number* (Social Security number, Passport number, Alien Number, and an encounter identifier); 3) *Address* (Full Address, Number, Street, Secondary Unit, City, State, Country, Postal Code); 4) *Incident* (Activity Number, activity description); and 5) *Biometrics* (booking photographs).

Only TECS Person Subjects annotated as a "suspect" and not as a victim or witness are shared. Information that is restricted by statute, regulation, or policy is filtered and not shared with member agencies. Examples of this type of information include:

- Protected Classes- (e.g., Asylum seekers; refugees; victim/witness; Violence Against Women Act, U, and T visa holders);
- Bank Secrecy Act information;
- Trade Secrets Act Information;
- National Security Information;
- Third Agency Information;
- Confidential Sources; and
- Undercover Operations.

How is the information accessed?

Information is accessed through a system-to-system interface. The LEIS Service uses the PRIME Interface Hub, a back-end tool, to transmit user queries to various DHS systems. Information that is queried using the PRIME Interface Hub is then returned through the LEIS Service and displayed through the member agency's user interface. While the PRIME Interface Hub has the ability to query a wide variety of DHS systems through the LEIS Service, data available for query is limited to those listed above.

How long is the information retained?

Information is not retained, as explained in Section I above.

Do DHS personnel have query capabilities to new data based on the MOA's?

No. Because this is a one-way query, DHS personnel cannot query records from these law enforcement partners and systems.