

GLOSSARY AT A GLANCE

Immigration Databases, Information Sharing Systems, and Case Management Systems

JANUARY 2018

THIS TABLE INTRODUCES THE VOCABULARY used by some federal and state databases and information sharing systems and federal investigative and case management systems that play a role in immigration enforcement. It does not aim to be comprehensive because the databases and systems are so numerous and the interrelationships among them so complex. Immigration enforcement depends not only on these databases and this technology — informal communications or collaboration between U.S. Immigration and Customs Enforcement (ICE) and state and local law enforcement officers or department of motor vehicle

employees also play an important role. We hope this table will help uncover the mystery behind some of these databases and systems, often known only by their acronyms.

A list of acronyms and abbreviations used in the table is provided on page 8. For more detailed information, see our report *Untangling the Immigration Enforcement Web: Basic Information for Advocates about Databases and Information Sharing Among Federal, State, and Local Agencies* (www.nilc.org/untangling-immigration-enforcement-web/).

NAME	DESCRIPTION	HYPERLINKS
U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP) Databases and Information Systems		
Alien Criminal Response Information Management System (ACRIME)	<p>According to DHS, “The Alien Criminal Response Management Information System (ACRIME) is an information system used by U.S. Immigration and Customs Enforcement (ICE) to support various law enforcement activities at the ICE Law Enforcement Support Center (LESC) and other ICE locations. ACRIME supports ICE’s handling of a response to immigration status Inquiries made by other agencies regarding individuals arrested, subject to background checks, or otherwise encountered by those agencies.</p> <p>“The system provides real-time immigration status determinations to federal, state, local, tribal, and international criminal justice agencies who submit Immigration Alien Queries (IAQ) to ICE. After receiving an IAQ, ICE uses ACRIME to research the subject of the IAQ, determine the immigration status of the subject, and generate an Immigration Alien Response (IAR) which is ultimately forwarded to the requesting criminal justice agency.”</p>	<ul style="list-style-type: none"> • https://www.archives.gov/files/records/mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2017-0002_sf115.pdf • https://www.dhs.gov/sites/default/files/publications/privacy-ICE-pia-020-b-acrime-january2013.pdf • https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-eidacrime-september2010.pdf

LOS ANGELES (Headquarters)
 3450 Wilshire Blvd. #108 – 62
 Los Angeles, CA 90010
 213 639-3900
 213 639-3911 fax



WASHINGTON, DC
 1121 14th Street, NW, Suite 200
 Washington, DC 20005
 202 216-0261
 202 216-0266 fax

NAME	DESCRIPTION	HYPERLINKS
	<p>ACRIME supports to the Secure Communities system (see description below). DHS reported in 2010 that it was combining ACRIME and Enforcement Integrated Database (EID) (see description below) data via the ICE Integrated Decision Support (IIDS) System, a reporting subsystem of EID.</p>	
<p>Automated Biometric Identification System (IDENT)</p>	<p>IDENT is a DHS-wide database where biometric information such as fingerprints (taken, e.g., when an individual applies for immigration benefits or is arrested on immigration charges) and associated biographical information are stored and are searchable. It is supposed to be replaced soon by a database with expanded biometric capabilities called Homeland Advanced Recognition Technology (HART).</p>	<ul style="list-style-type: none"> • https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013_0.pdf • https://www.federalregister.gov/documents/2016/12/15/2016-30187/supplemental-programmatic-environmental-assessment-spea-for-the-proposed-establishment-and • https://www.dhs.gov/sites/default/files/publications/DHS%20Biometrics%20%20Strategic%20Framework%20Webinar%20Slidedeck%20-%20October%2020%202015.pdf
<p>CBP Intelligence Records System (CIRS)</p>	<p>CIRS is a newly created system of records that was announced by DHS/CBP in a Sept. 21, 2017, System of Records Notice (SORN). According to the SORN, “CIRS contains information collected by CBP to support CBP’s law enforcement intelligence mission. This information includes raw intelligence information collected by CBP’s [Office of Intelligence], public source information, and information initially collected by CBP pursuant to its immigration and customs authorities. This information is analyzed and incorporated into intelligence products. CBP currently uses the Analytical Framework for Intelligence (AFI) and the Intelligence Reporting System (IRS) information technology (IT) systems to facilitate the development of finished intelligence products. These products are disseminated to various stakeholders including CBP executive management, CBP operational units, various government agencies, and the Intelligence Community (IC).” Public sources include “social media, news media outlets, and the Internet.” Government agencies include federal, state, local, as well as foreign agencies.</p>	<ul style="list-style-type: none"> • https://www.federalregister.gov/documents/2017/09/21/2017-19718/privacy-act-of-1974-dhscbp-024-intelligence-records-system-cirs-system-of-records
<p>DHS-Victim Information and Notification Exchange (DHS-VINE)</p>	<p>In April 2017, DHS launched the Victims of Immigration Crime Engagement (VOICE) office within ICE and announced the creation of DHS-VINE, “a free, confidential service that provides crime victims/witnesses, their family members, and victim advocates confidential notification of changes in custody status.” DHS-VINElink, the online portal to DHS-VINE, allows users to search for detainees (civil immigration incarceration) or in-state custody (criminal incarceration) and be notified of custody changes. DHS-VINElink builds on a commercially developed victim notification network in the criminal justice system called VINE.</p>	<ul style="list-style-type: none"> • https://www.dhs.gov/news/2017/04/26/dhs-announces-launch-new-office-victims-illegal-immigrant-crime • https://vinelink.dhs.gov/#/map • https://vinelink.com/#/home

NAME	DESCRIPTION	HYPERLINKS
Enforcement Integrated Database (EID)	EID is a DHS-wide database containing information related to the investigation, arrest, booking, detention, and removal of people encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and CBP.	<ul style="list-style-type: none"> https://www.dhs.gov/sites/default/files/publications/privacy_pia%20update_ice_enforcement%20integrated%20database_april%202014.pdf
ICEGangs	ICEGangs is an ICE database that serves as a repository of personal information about suspected or confirmed gang members and “associates,” as well as information on gang activities. ICE reportedly stopped using ICEGangs in 2016, because ICE agents were relying on other case management databases. ICE has not publicly announced this.	<ul style="list-style-type: none"> https://www.ilrc.org/sites/default/files/resources/ilrc_gang_advisory-20170426.pdf
LeadTrac	According to DHS, “LeadTrac is a database owned by the [HSI] Counterterrorism and Criminal Exploitation Unit (CTCEU). The function of LeadTrac is to vet and manage leads pertaining to visitors in the United States who are suspected of overstaying their period of admission or otherwise violating the terms of their admission, as well as organizations suspected of immigration violations.” Suspected status violators are referred to ICE field offices for investigation and enforcement. Information regarding NSEERS is maintained in LeadTrac.	<ul style="list-style-type: none"> https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-leadtrac-july2016.pdf, p. 1 https://www.regulations.gov/document?D=DHS-2016-0053-0001

DHS, ICE, and CBP Investigative and Case Management Systems

Analytical Framework for Intelligence (AFI)	<p>AFI is a CBP system that “provides enhanced search and analytical capabilities to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS at the border.”</p> <p>According to a 2016 Privacy Impact Assessment (PIA), AFI incorporates records from other CBP and DHS systems (including the National Security Entry Exit Registration System, or NSEERS) and has now added ICE and local law enforcement data sources, including providing access to the Law Enforcement Information Sharing Services (LEISS).</p> <p>According to the technology-focused website <i>The Verge</i>, “the system draws from a variety of federal, state, and local law enforcement databases that gather and analyze often-sensitive details about people, including biographical information, personal associations, travel itineraries, immigration records, and home and work addresses, as well as fingerprints, scars, tattoos, and other physical traits.” <i>The Verge</i> also reports that AFI no longer just allows access to other databases, but has instead become its own database, copying information it has obtained from other databases onto its servers.</p>	<ul style="list-style-type: none"> https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-010-a-afi-2016.pdf https://www.theverge.com/2016/12/21/14012534/palantir-peter-thiel-trump-immigrant-extreme-vetting
FALCON	<p>FALCON is an information technology platform developed by the private company Palantir. It has several components:</p> <ul style="list-style-type: none"> - FALCON Search & Analysis (FALCON-SA) - FALCON Tip Line (FALCON-TL) 	<ul style="list-style-type: none"> https://www.gpo.gov/fdsys/pkg/FR-2017-05-04/html/2017-09026.htm

NAME	DESCRIPTION	HYPERLINKS
	<ul style="list-style-type: none"> - FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS) - FALCON Roadrunner <p>According to a notice of Privacy Act exemptions, “In 2012, ICE HSI created a new IT environment called ‘FALCON’ to support ICE’s law enforcement and criminal investigative missions. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other Government [sic] applications and systems while employing appropriate user access restrictions at the data element level and robust user auditing controls.”</p> <p>FALCON-SA and FALCON-TL are described in more detail below.</p>	
<p>FALCON Search and Analysis (FALCON-SA)</p>	<p>Falcon-SA is a “consolidated information management system that enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE’s mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws.”</p> <p>FALCON-SA routinely ingests and allows users to query information from all the FALCON components, ICM, the Immigration and Enforcement Operational Records System (ENFORCE) — which includes ICE, CBP, and U.S. Citizenship and Immigration Services (USCIS) arrest and investigation records — and other ICE systems. On an ad hoc basis, FALCON-SA includes commercially available or public source data, criminal history information (including data from NCIC and state and local law enforcement), foreign government information, and more.</p>	<ul style="list-style-type: none"> • https://www.gpo.gov/fdsys/pkg/FR-2017-05-04/html/2017-09026.htm • https://www.dhs.gov/publication/dhsicepia-032a-falcon-search-analysis-system-falcon
<p>FALCON Tip Line (FALCON-TL)</p>	<p>According to a 2012 DHS/ICE PIA, FALCON-TL is a “workflow management system [that] supports the creation and maintenance of tips received by the HSI Tipline Unit about suspicious activity or suspected illegal activity, and the referral of this information to HSI field offices for appropriate investigation or other follow up.”</p> <p>The public and state and local law enforcement can submit tips via an online form or by phone. Once a tip is found to be “actionable,” it goes into FALCON-SA.</p>	<ul style="list-style-type: none"> • https://www.dhs.gov/sites/default/files/publications/ice-pia-033-falcon-tipline-2012.pdf
<p>ICE Pattern Analysis and Information Collection (ICEPIC)</p>	<p>According to a 2008 PIA, “ICEPIC is a set of information analysis tools which allow disparate sources of information to be analyzed to find previously unknown relationship data about individuals who are the subject of ongoing and valid investigations. Relationship data is made up of information about how a place, person, or thing (e.g., automobile or other piece of property) relates to other persons, places, or things.”</p> <p>According to a 2011 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.”</p> <p>A 2016 PIA regarding ICM said ICEPIC would be retired in 2016. It’s not clear if it has been.</p>	<ul style="list-style-type: none"> • https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_icepic-4a.pdf • https://www.gpo.gov/fdsys/pkg/FR-2008-08-18/html/E8-19031.htm • https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-pic-january2008.pdf

NAME	DESCRIPTION	HYPERLINKS
<p>Intelligence Reporting System (IRS)</p>	<p>The Intelligence Reporting System is referred to in several CBP documents but not defined. A 2017 PIA for the Intelligence Records System says that IRS and AFI technology systems are used “to facilitate the development of finished intelligence products.” The PIA reports that a PIA for IRS is forthcoming. It appears to have been in existence for some time, as it is referred to in a 2012 PIA for the Automated Targeting System.</p>	<ul style="list-style-type: none"> • https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf, p. 29 • https://www.federalregister.gov/documents/2017/09/21/2017-19718/privacy-act-of-1974-dhscbp-024-intelligence-records-system-cirs-system-of-records • https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf
<p>Investigative Case Management (ICM)</p>	<p>ICM is an information technology system/law enforcement management tool developed by the private company Palantir. It is used primarily by ICE Homeland Security Investigations (HSI) for criminal and civil prosecutions and investigations. ICE Enforcement and Removal Operations (ERO) can use ICM to manage criminal immigration cases and to query the system for information supporting civil cases.</p> <p>ICM allows ICE personnel to “create an electronic case file that organizes and links all records and documents associated with a particular investigation so they are easily accessible from a single location. It also enables personnel to link records to multiple investigations in order to draw connections between cases....”</p>	<ul style="list-style-type: none"> • https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/
<p>Law Enforcement Information Sharing Service (LEISS, sometimes abbreviated as LEIS)</p>	<p>According to DHS, “The Law Enforcement Information Sharing Service is a web-based data exchange platform, hosted by [DHS], that allows law enforcement agencies to rapidly share and access data related to criminal and national security investigations. ...</p> <p>“DHS law enforcement information is processed through the ICE Pattern Analysis and Information Collection System [hyperlink omitted] and includes information from subject records and closed cases concerning people, businesses, vehicles (including aircraft and seacraft [sic]), firearms and more.</p> <p>“The Law Enforcement Information Sharing Service currently provides federal, state, local, tribal and international law enforcement agency partners with access to more than 2.6 million subject records related to persons of interest, including suspects in child pornography, drug smuggling, immigration fraud, alien smuggling and a wide range of other cases.”</p> <p>DHS reports on its website that it has deployed the service “on a regional basis in San Diego, Los Angeles, Seattle, Arizona, and Texas. In addition, the U.S. Department of Justice established connectivity to the service via the OneDOJ program” [hyperlink omitted].</p>	<ul style="list-style-type: none"> • https://www.ice.gov/le-information-sharing

NAME	DESCRIPTION	HYPERLINKS
U.S. Department of Justice (DOJ) Databases		
Interstate Identification Index (III)	Per 28 CFR 20.3(m), the Interstate Identification Index system, or III system, is “the cooperative federal-state system for the exchange of criminal history records, and includes the National Identification Index, the National Fingerprint File, and, to the extent of their participation in such system, the criminal history record repositories of the states and the FBI.” The III system is maintained by the FBI (Federal Bureau of Investigation).	<ul style="list-style-type: none"> • https://www.law.cornell.edu/cfr/text/28/20.3. See https://www.fbi.gov/file-repository/interstate-identification-index-iii-national-fingerprint-file-nff.pdf/view for participating states.
National Crime Information Center (NCIC)	NCIC is an FBI database containing “an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year.” Despite the FBI’s description of the NCIC as a criminal database, it also contains civil immigration information, such as information regarding persons with outstanding immigration removal orders and persons designated as “criminal aliens” who have been deported. It also includes a Gang File.	
Next Generation Identification (NGI)	<p>NGI is an expanded FBI biometric database (including fingerprints, iris prints, palm prints) with advanced services, including a facial recognition system and ongoing status notification of criminal history. It replaces the Integrated Automated Fingerprint Identification System (IAFIS).</p> <p>NGI also offers services such as the Repository for Individuals of Special Concern (RISC), which allows law enforcement to take fingerprints in the field using mobile devices and to check them against the NGI databases, getting responses in a matter of seconds. The NCIC’s Immigration Violator File can be checked through the RISC.</p>	<ul style="list-style-type: none"> • https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi • https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis-ngi-risc • https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi
Interoperability Between DOJ and DHS Databases		
Secure Communities (S-Comm)	Under S-Comm, a fingerprint check of arrested persons against FBI databases results in an automated check (interoperability) against DHS databases. The system notifies ICE when there is a “hit,” and ICE then determines whether to take enforcement action against the individual arrested.	<ul style="list-style-type: none"> • https://www.ice.gov/secure-communities
State Databases and Information Sharing Systems		
GangNet	<p>GangNet is a commercial intranet-linked software that offers a database with information and photos on individuals and gangs, data analysis, facial recognition software, mapping, a field interview form, and a watch list. Using a single command, agencies can simultaneously search their own GangNet system and a network of GangNet systems in other states and federal agencies.</p> <p>The GangNet software is operational in many states (Arizona, California, District of Columbia, Florida, Georgia, Maryland, Minnesota, Nevada, New Mexico, North Carolina,</p>	<ul style="list-style-type: none"> • http://www.law.uci.edu/academics/real-life-learning/clinics/ucilaw-irc-MislabeledReport.pdf • https://assets.documentcloud.org/documents/1683801/gangnet8-whitepaper2013.pdf

NAME	DESCRIPTION	HYPERLINKS
	<p>South Carolina, Texas, Virginia, Washington), as well as in Canada. ICE, the FBI, and the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) are also connected to it and able to share information in real time.</p>	
<p>Nlets</p>	<p>Nlets is a state-owned telecommunications network and describes itself as “the premiere interstate justice and public safety network in the nation for the exchange of law enforcement-, criminal justice-, and public safety-related information.” It is used by criminal justice agencies in U.S. states and territories, federal criminal justice agencies including ICE, and some international agencies. Data that can be exchanged through Nlets includes criminal histories, motor vehicles and driver’s license and driving history data, and much more. Currently many states share driver’s license photos through Nlets.</p>	<ul style="list-style-type: none"> • http://www.nlets.org/about/who-we-are • See http://www.nlets.org/our-members/grantmaps?mapid=d26b4e70-934e-11e3-9a61-00155d003202 for driver’s license photo-sharing map
<p>State criminal justice databases</p>	<p>States have their own criminal justice networks that collect and share information related to their criminal justice systems and their departments of motor vehicle (DMVs). For example, in Connecticut, the Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT) system includes state criminal history and DMV records, as well as other state databases, and provides access to databases in other states as well as databases administered by the U.S. and Canada through Nlets and NCIC.</p>	<ul style="list-style-type: none"> • http://www.ct.gov/cjis/cwp/view.asp?a=4103&q=480592
<p>State department of motor vehicles (DMV) databases</p>	<p>Though state DMV databases differ from state to state, in general they contain information provided in obtaining a driver’s license or that appears on the face of a license, driver’s license photographs, car registration information, car insurance information, and traffic offense information.</p> <p>ICE obtains information in state DMV databases through Nlets, state criminal justice databases, and informal communications between ICE and DMV employees.</p>	<ul style="list-style-type: none"> • www.nilc.org/ice-dmvs-share-information/

ACRONYMS & ABBREVIATIONS USED IN THE TABLE

ACRIME – Alien Criminal Response Information Management System

AFI – Analytical Framework for Intelligence

ATF – U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives

CBP – U.S. Customs and Border Protection

CIRS – CBP Intelligence Records System

COLLECT – Connecticut On-Line Law Enforcement Communications
Teleprocessing

CTCEU – HSI Counterterrorism and Criminal Exploitation Unit

DHS – U.S. Department of Homeland Security

DHS-VINE – DHS-Victim Information and Notification Exchange

DMV – department of motor vehicles

DOJ – U.S. Department of Justice

EID – Enforcement Integrated Database

ENFORCE – Immigration and Enforcement Operational Records System

ERO – ICE Enforcement and Removal Operations

FALCON-DARTTS – FALCON Data Analysis & Research for Trade
Transparency System

FALCON-SA – FALCON Search & Analysis

FALCON-TL – FALCON Tip Line

FBI – Federal Bureau of Investigation

HART – Homeland Advanced Recognition Technology

HSI – ICE Homeland Security Investigations

IAFIS – Integrated Automated Fingerprint Identification System

ICE – U.S. Immigration and Customs Enforcement

ICEPIC – ICE Pattern Analysis and Information Collection

ICM – Investigative Case Management

IDENT – Automated Biometric Identification System

III – Interstate Identification Index

IRS – Intelligence Reporting System

IT – information technology

LEIS – See LEISS

LEISS – Law Enforcement Information Sharing Services (sometimes
referred to as LEIS)

NCIC – National Crime Information Center

NGI – Next Generation Identification

NSEERS – National Security Entry Exit Registration System

PIA – Privacy Impact Assessment

RISC – Repository for Individuals of Special Concern

S-Comm – Secure Communities

SORN – System of Records Notice

USCIS – U.S. Citizenship and Immigration Services

VOICE – Victims of Immigration Crime Engagement