Privacy Impact Assessment

for

ICE Investigative Case Management

DHS/ICE/PIA-045

June 16, 2016

Contact Point

Peter T. Edge

Executive Associate Director

Homeland Security Investigations

U.S. Immigration & Customs Enforcement

(202) 732-5100

Reviewing Official

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717

Abstract

U.S. Immigration and Customs Enforcement (ICE), a component agency within the Department of Homeland Security (DHS), is establishing a new, major Information Technology (IT) system known as Investigative Case Management (hereafter, ICM). ICM is replacing ICE's use of the case management module in Legacy TECS[1] (hereafter, TECS), a system developed in 1987 by the former U.S. Customs Service and currently administered by U.S. Customs and Border Protection (CBP), another component within DHS. ICE is conducting this Privacy Impact Assessment (PIA) to document the privacy protections that are in place for the personally identifiable information (PII) contained in ICM as well as the following inter-related capabilities: 1) an Interface Hub to control the movement of information between most ICM and external information repositories; 2) the HSI Data Warehouse to store case information for the purpose of facilitating information sharing and reporting; and 3) the Telecommunications Linking System (TLS) (and its interface with Pen-Link), which will store case-related telecommunications information.

Overview

ICE developed ICM to support its mission to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. ICM serves as the core law enforcement case management tool primarily used by ICE Homeland Security Investigations (HSI) special agents and personnel supporting the HSI mission. HSI conducts domestic and transnational criminal investigations to protect the United States against threats to national security, to prevent the illicit cross-border movement of goods, people, and monetary instruments, and to bring to justice those seeking to exploit U.S. customs and immigration laws worldwide. Additionally, ICE Enforcement and Removal Operations (ERO) personnel use ICM to manage immigration cases that are presented for criminal prosecution under U.S. Code Title 8 - Aliens and Nationality, and U.S. Code Title 18 - Crimes and Criminal Procedure. ERO will also use ICM to query the system for information that supports its civil immigration enforcement cases. The ICE Office of Professional Responsibility (OPR) has read-only access to ICM as well as audit capability to conduct internal administrative or criminal investigations related to misconduct and/or misuse of ICM. Certain attorneys in the ICE Office of

[1] DHS/CBP/PIA-009 – TECS System: CBP Primary and Secondary Processing: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf

the Principal Legal Advisor (OPLA) also have read-only access to the system in support of their work on mission-related matters.

ICE HSI personnel are the primary users of ICM, but ICE personnel working in ERO and OPR, as well as some ICE attorneys who support these programs, also have access to and use the system, as explained below. Like its predecessor case management system in TECS, ICM enables 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, which enhances the investigative process and facilitates coordination and deconfliction.[2]

The primary functions of ICM are as follows:

- Create and manage ICE HSI criminal and civil investigative case files and certain ERO criminal investigative case files. These case files will include Subject Records, Reports of Investigation, and other case documents.
- Link Subject Records and case documents within and between investigations to ensure users have a comprehensive view of all activities and subjects related to a single case.
- Enable effective case deconfliction and coordination between personnel working connected investigations.
- Ensure continuity of current information sharing with CBP in support of the related missions of ICE and CBP.
- Perform investigative research via system interfaces both internal and external to ICE and DHS.
- Create and manage law enforcement statistics (e.g., arrests and seizures) and capture administrative data (e.g., agent work hours on cases) for management and reporting purposes.

ICM Users

All ICM users are ICE personnel or individuals with a need to know who are either detailed to ICE or assigned to an ICE-led task force. ICM's primary purpose is to support HSI's exercise of its broad legal authority to investigate and enforce a diverse array of federal criminal laws. HSI uses this authority to investigate all types of cross-border criminal activity to protect the United States against threats to national security and to bring to justice those seeking to exploit U.S. customs and immigration laws worldwide. The scope of HSI investigative authority includes financial crimes, money laundering, and bulk cash smuggling; commercial fraud and intellectual

[2] Deconfliction is the identification of previously unknown connections amongst investigations; for example, when agents review call records and discover that the targets of two separate investigations have phoned the same number.

property theft; cybercrimes; human rights violations; human smuggling and trafficking; immigration, document, and benefit fraud; narcotics and weapons smuggling/trafficking; transnational gang activity; export enforcement; and international art and antiquity theft. HSI documents and manages its investigative activities in ICM. In addition to criminal investigations, HSI uses the system to manage its civil law enforcement activities and to support criminal prosecutions arising from its investigations.

ERO uses ICM in a more limited way than HSI in support of its mission to enforce U.S. immigration laws by identifying, arresting, and removing aliens in a way that is consistent with current enforcement priorities.[3] ERO uses ICM as a case management system only for those immigration cases that are presented for criminal prosecution under U.S. Code Title 8 - Aliens and Nationality, and U.S. Code Title 18 - Crimes and Criminal Procedure. ERO personnel also query ICM as needed for information related to their immigration enforcement cases, which are civil in nature. ERO will continue to use the Enforcement Integrated Database (EID) to manage its civil cases.[4]

OPR is the agency's internal affairs office, and uses ICM in a limited way as well. OPR upholds the agency's standards for integrity and professionalism. As a key part of that responsibility, OPR investigates allegations of employee misconduct. OPR personnel have read-only query access to ICM in support of their administrative and criminal investigations and direct access to the HSI Data Warehouse. During the course of OPR investigations of suspected misconduct, they also review audit log files that capture ICM and HSI Data Warehouse user activity. OPR does not use ICM as a case management system, but will continue to use the Joint Integrity Case Management System,[5] which is owned and administered by CBP, for that purpose.

Some OPLA attorneys have access to ICM in support of their work on mission-related matters including, but not limited to, representing DHS in exclusion, deportation, and removal proceedings; arguing administrative appeals before the Board of Immigration Appeals; and providing direction and support to Offices of the United States Attorneys. OPLA users have read-only access to the system. They are not able to create or modify records in ICM.

Modernization of Legacy TECS

TECS was developed in 1987 by the former U.S. Customs Service and has been administered by CBP since DHS was created in 2003. It was an information sharing and case

[3] DHS currently prioritizes for enforcement actions those aliens who present a danger to national security or are a risk to public safety, as well as those who enter the United States illegally or otherwise undermine the integrity of U.S. immigration laws and border control efforts.
[4] DHS/ICE/PIA-015 Enforcement Integrated Database (EID): https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf
[5] The ICE data contained in JICMS is covered by the DHS/ALL-020 Department of Homeland Security Internal Affairs SORN (April 28, 2014, 79 FR 23361), available at https://www.gpo.gov/fdsys/pkg/FR-2014-04-28/html/2014-09471.htm

management platform that allowed users to access different databases that were maintained on the platform or accessed through the platform. ICE used the case management module in TECS to document its law enforcement investigations and support criminal prosecutions.

Because of its age, TECS did not provide a modern interface for users or up-to-date security features and, in many cases, was no longer supported by hardware and software vendors. Thus, ICE and CBP began parallel and collaborative modernization efforts with the goal of retiring TECS in 2016. Through a joint governance process, both DHS components are replacing TECS with separate systems that interface to ensure current data sharing between ICE and CBP continues.

The ICM System includes the ICM application, which provides the case management capabilities, and three inter-related capabilities: 1) an Interface Hub to control the movement of information between ICM and external information repositories; 2) the HSI Data Warehouse to store case information for the purpose of facilitating information sharing and reporting; and 3) the TLS application (and its interface with Pen-Link), which will store case-related telecommunications information obtained via subpoena or other means.

ICM Application

The ICM application is built on a customized platform that enables the creation and management of comprehensive case files and provides improved functionality over the case management module in TECS. These improvements include: 1) an updated user interface that simplifies user interactions; 2) enhanced search capabilities that allow for the use of both structured and unstructured queries regarding subjects of interest; 3) deconfliction of data so that each subject has one consolidated record; 4) workflow capabilities to support internal case review and approval; and 5) enhanced collaboration within ICE.

The user interface for the ICM application is an internal web-based front-end. The ICM application uses Single Sign-On (SSO) to validate ICE users with Personal Identity Verification (PIV)-card authentication. SSO is a method of access control that enables a user to log in at a single point and gain access to the resources of multiple software systems by using credentials stored on shared, centralized authentication servers. PIV-card authentication provides an extra layer of security by storing a user's SSO credential on a physical card that must be present at login.

ICM contains extensive information related to individuals including targets of investigations, associates of targets, victims, informants, and other third parties. This includes biographical and descriptive identifying data, as well as information about individuals' locations and activities. More details about this information may be found in section 2.1.

ICM maintains comprehensive case files that contain Subject Records and case documents. There are six types of Subject Records—Person, Business, Vehicle, Vessel, Aircraft, and Thing.[6]

[6] For more information on Subject Records, please see the DHS/CBP/PIA-009 – TECS System: CBP Primary and

Any Subject Record or case document may be linked to a case file, another Subject Record, or another case document within the system. This ensures all investigative information related to a subject is available to ICM users, and supports coordination and deconfliction between cases. Case documents include but are not limited to Reports of Investigation (ROIs), evidence, court records, and incident reports including arrest reports, seizure reports, and electronic surveillance reports (ELSURs). ROIs are narratives documenting investigative activities. ROIs may describe case details and statuses, summaries of events (e.g., target encounters, witness or victim interviews, surveillance activities), agent observations, descriptions of evidence, and any other information relevant to a case. ICM also has the ability to retain media files, including video and still images.

ICM users are given role-based permissions, and each ICM user has an individual "desktop" in the application with the top-level view presenting links to all of the case files for that user's assigned cases. The user is able to create and/or upload and link Subject Records and case documents using simple drop-down menus, and has access to extensive search capabilities from most places within the system. When a user accesses a case file, all Subject Records and documents that have been linked to that case are accessible. A user may also create a Subject Record and leave it unlinked until its association with a case or other record is clear. Users who are provisioned as supervisors in the system are able to view all of the case files created by their subordinates. Supervisors have access to additional functionality, as well, such as the ability to approve or reject ROIs or other records and documents produced by their subordinates.

The ICM application is intended to help ICE agents and officers identify related investigations to ensure they are properly coordinated and the respective investigative teams do not inadvertently interfere with one another's work. To this end, ICM users receive alerts within the system when their investigative records are accessed by another user. An exception exists for OPR users, who can access records without generating an alert. These alerts inform the owner of the record (typically the case agent) which other user has accessed the record so that the owner may connect with that user to determine whether coordination is needed. By default, ICM records are visible to all other ICM users to promote deconfliction and coordination of law enforcement work. This process is discussed in further detail in section 3.4. However, when appropriate, ICM users may limit the visibility of records related to certain sensitive investigations to only a subset of users. Limiting in this manner may occur in a particularly sensitive investigation when it is appropriate for only the team of agents engaged in the case and their supervisors to have access to the case materials. To ensure accountability, however, supervisors always have the ability to see the records and cases their subordinates create. Additionally, all ICM user activity, including OPR activity, is tracked in audit logs.

Secondary Processing: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf.

Interface Hub

The Interface Hub is a custom back-end tool that automatically transmits queries from ICM to other information systems both internal and external to ICE and returns results back to ICM.[7] These systems are detailed in section 2.2, and generally include ICE and other Federal Government databases containing information on subjects, seizures, arrests, and immigration and criminal history data. Depending upon the system and circumstances, ICM users who are conducting law enforcement investigations can generate queries from within the system and either import the query results into ICM (e.g., import to a case file the target's arrest report obtained from EID), or manually review the query results and then copy and/or describe the information in an ICM record, generally an ROI. For example, through the Interface Hub, ICM users are able to query the system CBP is creating to replace its portions of TECS, called the CBP TECS Platform[8], for data relevant to their investigations and elect to directly import results into ICM to create a master Subject Record, if one does not already exist or to create a sub-record to an existing master Subject Record. When data is imported directly to create a record, it is date-stamped. The source for the import is apparent based on the type of record. When ICM users copy or describe information from other sources, they note the source for the information within the relevant record. ROIs are ony available to ICM users once they are approved, and the approval date is visible to other users. Therefore, users who might rely on information in an ROI are aware that the information was current at the time of approval.

Finally, the Interface Hub allows ICM to continually publish and update ICE-created Subject Records to the CBP TECS Platform, which ensures that CBP continues to have access to ICE Subject Records as they did in the TECS system. These ICE Subject Records, which are typically about targets of ICE law enforcement interest (e.g., individuals, vehicles, and aircrafts), serve as "lookout records" that assist CBP personnel in conducting screening at exit and entry at U.S. borders.

HSI Data Warehouse

The HSI Data Warehouse is a data storage environment that serves as a repository for ICM system data. It receives a direct feed once every 24 hours containing a refresh of ICM data, including new records and edits to previously existing records. The HSI Data Warehouse supports reporting and the export of data once every 24 hours to ICE's FALCON Search & Analysis System (FALCON-SA)[9]. Having these functions supported by the HSI Data Warehouse improves the functioning and speed of the ICM application by allowing it to be used exclusively for real-time

[7] There is no direct user interface for the Interface Hub; instead its functions are integrated into the user interface of the ICM application.
[8] The CBP TECS Platform provides a web-based user interface that enables CBP users to access the new CBP TECS backend database. For more information, see the forthcoming CBP TECS Platform PIA.
[9] DHS/ICE/PIA-032(a) FALCON Search & Analysis System (FALCON-SA): http://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf

case management.

Some ICE personnel, such as employees from HSI's Executive Information Reporting Unit (EIRU), HSI and ERO supervisors, and OPR will have direct user access to the HSI Data Warehouse that is separate from access to the ICM application. HSI Data Warehouse users (all of whom are ICE personnel) access the repository via an internal web-based interface and are validated using SSO with PIV-card authentication. All users are able to generate and access a variety of read-only reports derived from ICM data (e.g., summaries of hours, arrests, or seized items per office per fiscal year; numbers of search warrants per case). EIRU users are able to customize reports to satisfy ICE leadership, congressional, and other requests, as appropriate. All HSI Data Warehouse user activity is tracked in audit logs.

FALCON-SA receives an export from the HSI Data Warehouse of the same ICE-owned data that FALCON-SA historically received from TECS. This includes Case Summaries, ROIs, Subject Records, and other case-related material. These records and the PII contained in them are described in more detail in section 2.1 below.

TLS and Pen-Link

The Telecommunications Linking System (TLS) (previously a subsystem of TECS) is an application within the ICM environment, and is HSI's national repository of case-related telecommunications information derived from any type of investigative law enforcement case or event. This data is usually obtained via a subpoena to a telecommunications company (e.g., phone company) and contains transactional details about telecommunications activities. It does not contain the contents of any communications. TLS contains telecommunications information initially input into ICE's Pen-Link software, which serves as a field-level investigative tool enabling HSI to perform local analysis within a single case or across multiple cases. Pen-Link contains a custom module built for ICE that standardizes the telecommunications records from the myriad formats used by service providers and is used to export and import data files in a specific format that is used by TLS. TLS links related data by using key identifiers for this telecommunications information, such as phone numbers. This linkage enables HSI agents to discern relationships that may help to identify the parties of criminal networks under investigation, promoting further investigation and contributing to the eventual disruption or dismantling of the criminal organizations. It can also serve to help HSI agents to deconflict cases; that is, to identify previously unknown connections between investigations.

Data imported into TLS is associated with one or more case identification numbers. When an HSI agent searches TLS from within ICM, any agents whose cases are linked to the queried information by the case identification number receive an alert that provides the information of the agent who initiated the query. For example, the telecommunications data in TLS may identify that the target of an investigation in a Seattle case is calling a target in a case in Houston, and alert both case agents that their investigations are likely related. TLS records are broken down into three

categories: call, subscriber, and miscellaneous records. These categories are further explained in Question 2.1. FALCON-SA also ingests TLS data directly from TLS on a nightly basis for analysis and further deconfliction.

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?

Pursuant to the Homeland Security Act of 2002 (P.L.#107-296, Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include, but are not limited to, laws residing in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this authority to 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).

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

ICM data is covered under the existing DHS/ICE-009 External Investigations SORN.[10]

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

Yes. ICM and the HSI Data Warehouse have each completed Security Control Assessments, and each will receive an Authority to Operate (ATO) by June 20, 2016. The ICM ATO will also cover TLS, and the HSI Data Warehouse ATO includes the Interface Hub.

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

No, ICE is in the process of scheduling ICM and TLS records.

[10] DHS/ICE-009 External Investigations SORN (January 5, 2010, 75 Fed. Reg. 404).

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.

Nearly all information collected and maintained in ICM is in support of a criminal investigation. Because the collection of information for purposes of a criminal investigation is exempt from the requirements of the Paperwork Reduction Act, the majority of the information in ICM is not covered by the PRA. However, ICM contains information pertaining to ICE's audits of employers related to their compliance with the creation of Form I-9s (OMB No. 1615-0047). This form is subject to the PRA and is owned and published by U.S. Citizenship and Immigration Services.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

Information on the following categories of individuals is contained within ICM: targets of investigations, associates of targets, victims, witnesses, informants, and other third parties (e.g., a person who reports a crime, an individual whose identity is used by a target, an employer). PII is contained in case documents, such as ROIs, Person Subject Records, and may also appear in the other five types of Subject Records.[11] For example, a Vehicle Subject Record may contain the name and address of the person to whom the vehicle is registered. Targets of investigations will always have unique Person Subject Records in ICM. Other individuals related to an investigation may have unique Person Subject Records or their information may appear in another Subject Record.

The types of information contained in ICM Subject Records and case records, such as ROIs, include:

- *Biographic data* including but not limited to name, alias, date of birth (DOB), Social Security number (SSN), Alien Registration Number, address, phone number, driver's

[11] The other five types of Subject Records are Business, Vehicle, Vessel, Aircraft, and Thing.

license number, passport number, pilot's license number, criminal history, and immigration status and history.

- *Descriptive data* including eye color, hair color, height, weight, and any other unique physical characteristics (e.g., scars, marks, tattoos).
- *Financial data* including data on suspicious financial activity, currency transaction reports, and currency or monetary instrument reports.
- *Evidence and descriptions of evidence obtained during an investigation* including but not limited to statements of targets and witnesses, photographs, emails, phone records, banking records, travel history records, and other related documents. This may include photographs, videos, audio, maps, and other visual representations of information. Depending on the nature and volume of the evidence, it may be scanned and linked to other records in the system, or excerpts from the source documents of large amounts of data (e.g., boxes of files) may be cited. Evidence may also include physical items (e.g., narcotics or firearms) that are lawfully seized, documented, and stored in ICE evidence rooms for use during a prosecution. Descriptions and photographs of these items may be uploaded as case documents in ICM. Depending upon the circumstances, any materials described above may contain PII.
- *Location-related data*: Most location data in ICM comes from agent or officer observations during surveillance activities or witness accounts. ICM may also contain specific types of location data from surveillance tools and technologies, as described here:
  - Location tracking tools. During the course of criminal investigations, HSI uses various technologies to support the location tracking of individuals, vehicles, and contraband. The location tracking tools themselves, which include covert tracking devices, do not store identity information about an individual nor do they maintain a list of individuals who are the targets of HSI investigations. The tools only maintain a list of tracking devices by serial number/Mobile Directory Number (MDN)/International Mobile Equipment Identity (IMEI)/Mobile Equipment ID (MEID), etc., and their current locations using GPS and/or assisted Cellular Tower coordinates. This information is stored on an ICE server and accessed by HSI agents via an internal web-based portal that presents location data of tracking devices related to their investigations in a graphical view (real-time maps). The tools are deployed on targets of investigations, vehicles of interest in investigations, but also on the official vehicles owned by ICE and used by agents and officers in the field. The case agent tracks the device information along with the identifying information of the individual, vehicle, or other object being tracked in the agent's investigative case notes, which are stored outside of ICM. However, HSI agents

may enter location data, including tracking device numbers, in case documents such as ROIs, and may also upload spreadsheets containing this information as case documents in ICM.

- License plate reader (LPR) data. ICM may contain limited location data from LPR cameras operated by ICE and placed for surveillance during a particular investigation, or obtained as a result of joint initiatives with law enforcement partners (e.g., federal, state) with access to LPR databases containing data collected only from law enforcement sources. This data includes images of vehicles license plates associated with a target of investigation (a person or vehicle), date and time, and GPS coordinates for the location where the license plate was photographed. The sources for this data are detailed in section 2.2. ICE personnel may upload the images into ICM as case documents and link them to Subject Records. They may also describe this information and any related actions in arrest reports, other incident reports, or ROIs. LPR data is documented only in the context of individual case files within ICM.

- *Telecommunications data:* The TLS application within the ICM system contains telecommunications information, standardized by and uploaded from Pen-Link, that may contain PII. ICE collects the data in TLS pursuant to administrative subpoenas and court orders, as required by law. This data includines telecommunication device identifiers, telecommunications usage data, and biographic information on targets of investigations, potential targets, associates of targets, or any individuals or entities that receive calls from these individuals. Telecommunication device identifiers include telephone numbers, International Mobile Subscriber Identity (IMSI), Universal Fleet Member Identity (UFMI), Electronic Serial Number (ESN), email address, Universal Resource Locator (URL), and Internet Protocol (IP) addresses. Telecommunications usage data consists of telephone call information (date/time, duration, dialed number, etc.). Biographic information consists of names, addresses, telephone numbers, DOB, SSN, or passport number of any person identified as the subscriber, registered customer, or known user of a telecommunications device. TLS does not contain the content of any communications. TLS contains three types of records:

  - Call records contain call detail transaction information of telephone calls and in some cases text messages. Information in call records includes the originating and receiving telephone number (or IP address); the date, time, and duration of each call; and the number of calls between those two numbers. Depending upon the source of the information, originating and terminating cell tower location information may be included with the call record.

- Subscriber records may contain telephone numbers, IP addresses, subscriber names and aliases, information about associates, addresses, biographic information as described above, mobile device identifiers, information about how the data was obtained (e.g., subpoena), associated ICE case ID numbers, dates associated with the creation and update of any subscriber data, any information about the relationship between the subscriber and the case or case target (e.g., target's dentist office). These records are entered by HSI agents or analysts based on information they obtain via investigative means about the individuals who are making and receiving the calls in question. They are generally based on identified and authoritative sources; for example, information from a service provider or a registered informant.
- Miscellaneous Records are manually created by agents and contain the same types of information as subscriber records, except their source may be unknown or unverified. An example of a source that would lead to the creation of a miscellaneous record in TLS is the collection of a phone book from an arrested individual during a search of their "pocket trash." The investigating agent may input the names and phone numbers of individuals in the suspect's phone book as miscellaneous records associated with the agent's case, thereby allowing TLS to use this data to link to call records where calls may have been made to or from that number.

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

ICE collects information from a wide variety of internal and external sources that will be placed in ICM during the course of ICE criminal and civil law enforcement investigative activities.

Agent/Officer Observations and Surveillance Activities:

A large amount of investigative information comes from agent or officer observations and surveillance activities. ICM users document these observations and activities primarily in ROIs. The vast majority of ICE's surveillance activities are physical (i.e., agent) observations. Some other examples are as follows:

- HSI agents will sometimes set up pole cameras to record individuals entering and exiting a specific location where there is suspected criminal activity. The agent's description of the probative video footage would be documented by that agent in an ROI, and the footage, itself, may be uploaded to ICM.
- Agents may conduct electronic surveillance, such as a monitored/recorded phone call or videotape of a meeting between a target and an undercover agent. These activities are

generally conducted when one party (e.g., an agent, cooperating defendant, or confidential informant) has consented to the monitoring. The electronic surveillance is first documented in ICM with an ELSUR, which also officially serves as the agent's request to a supervisor to conduct the surveillance. ELSURs are approved at the HSI headquarters level. Once HSI headquarters approves the ELSUR and the agent conducts the surveillance, the agent documents the activity in an ROI and also appends the ELSUR with one or more Reports of Use, which include brief details of each contact resulting from the surveillance.

Individuals

Some of the investigative data contained in ICM comes from targets of investigations, associates of targets, victims, registered informants, and other third parties who are questioned or interviewed during the course of an investigation. This includes information obtained from documents provided by or retrieved from individuals. Information collected from these sources may be found in Subject Records or case documents. For example, an agent may document the information collected in an informant interview in an ROI. The agent may also learn of a previously unknown criminal associate during this interview and create a new Subject Record with that information. Alternatively, the agent may be given an item or document by an individual (e.g., a photograph or receipt) and summarize and/or upload a copy of the document into ICM.

ICE location tracking projects and technologies

ICM users may obtain location data pertaining to a person or object of interest in an investigation using existing ICE tools located outside of ICM, as well as information obtained via partnerships with other law enforcement agencies. HSI agents have access to a vendor application separate from ICM via a web-based portal that presents location data of tracking devices in a graphical view (real-time maps). An ICE server accepts and stores covert tracking device location data from various satellite and cellular service providers and transmits the data to a separate application internal to ICE (also a third-party product) that generates the maps. This third-party application and its data does not contain any information identifying a specific individual (e.g., individual name) or the investigative case number. It is also not connected to any DHS network so it cannot exchange information with ICM or other systems. The vendor application allows HSI agents and supporting investigative personnel to view the unique alpha-numeric identification number for a tracking device, the date and time that a location was recorded, and the GPS coordinates for that location. HSI agents and supporting personnel have access only to information about the tracking devices related to their own investigations and may associate the device information with a target in ICM by manually inputting the data they obtain from the application in Subject Records or case documents. The application allows exporting of current and historical information for a location tracking device to a spreadsheet, which may be uploaded into ICM as a case document and linked to an existing ICM record.

ICM users may also obtain location data via use of LPR technology in two ways.[12] First, ICE may deploy ICE-owned LPR cameras to conduct surveillance at locations relevant to a criminal investigation. This use of LPR technology is location-centric, as it focuses on a given location of interest to the case. This could be a smuggling route or a location outside of a business where the investigative target is known to frequent, for example. These cameras capture license plate images and the date/time and location of the capture. The storage devices associated with these cameras are stand-alone and do not network with any databases or systems. Agents will document any relevant information obtained via the surveillance, including the license plate numbers of interest, in appropriate case documents within ICM, such as an ROI. The raw data typically is deleted off of the storage device associated with the camera, although in some cases images of license plates may be uploaded to the ICM case when they pertain to a target or associate. ICE does not retain or share data and images related to license plates that are not related to the immediate case.

ICE also may obtain location data via associations with other law enforcement agencies or task forces that collect and use LPR technology, such as from CBPs LPR cameras at ports of entry[13] or through established partnerships with federal, state, and local law enforcement agencies (e.g., High Intensity Drug Trafficking Area task forces). The information to which ICE has access as a result of these partnerships is collected only from law enforcement sources. This use of LPR technology is vehicle-centric, as it focuses on a given vehicle of interest to the investigation. This could be a vehicle known to be owned or operated by a target, or a vehicle believed to be smuggling contraband, for example. Typically, ICE law enforcement personnel will be able to add license plates of interest to a criminal investigation to a "hot list" within the LPR system owned by its partner(s). These hot lists are uploaded by ICE personnel and are not made available to the law enforcement partners that own the databases. When a license plate on a hot list is captured by a camera linked to the database, the ICE agent with whose investigation that license plate is associated receives an automated email notification. The notification typically provides an image of the license plate number, computer-generated text of the information the software has read from the license plate, and the GPS coordinates for the location where the license plate was photographed. The purpose of these notifications is to provide agents with real-time location

[12] The LPR data sources described in this PIA differ from the sources covered by the DHS-ICE-PIA-039 – Acquisition and Use of License Plate Reader Data from a Commercial Service, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf. That PIA described the privacy risks and management strategies associated with ICE's intention to procure access to commercial license plate reader databases. The commercial enterprises that maintain these databases may collect LPR data from both private and public contributors, including law enforcement agencies, parking garages, and repossession companies. They make this data available on a fee-for-service basis to both public and private entities. The LPR data described here is obtained directly by ICE or by other law enforcement agencies, typically from targeted, strategic locations, and provided only to ICE and other law enforcement agencies in support of investigative and enforcement activities.

[13] For more information on CBP's use of LPR cameras at ports of entry, please see the DHS/CBP/PIA-009 – TECS System: CBP Primary and Secondary Processing: https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf

information so that they may take action, if appropriate. Agents may upload the images and/or copies of the notifications into ICM as case documents and link them to Subject Records. They may also describe this information and any related actions in arrest reports, other incident reports, or ROIs. ICE enters into these partnerships pursuant to terms detailed in Memoranda of Agreement and agents who have access to this information are required to comply with ICE Rules of Behavior covering access to and appropriate use of the data. Among other requirements, the ICE Rules of Behavior include limitations on the use of the data (i.e., only for authorized law enforcement purposes), strict criteria for creating alerts, a prohibition on *ad hoc* and historical queries, specified timeframes for refreshing alerts, and a requirement to manually verify the accuracy of data contained within notifications.

Telecommunications data in TLS

The telecommunications information loaded into Pen-Link and then TLS comes from various sources to include but not limited to call information from lawful intercepts such as Title III intercepts and pen registers; telephone billing, call detail and subscriber information obtained from service providers by subpoena, summons, or court order; informant information; seized address books, notes, pocket trash, and other documents.

DHS and other federal agencies

During the course of an investigation, ICE may also collect information from paper or electronic federal records from other DHS components including but not limited to CBP, U.S. Citizenship and Immigration Services, Transportation Security Administration, and U.S. Coast Guard. This may occur via queries to the systems maintained by these other components to which ICE has user access, or via manual requests made to component personnel. ICE requests and collects this information from its DHS partners pursuant to section (b)(1) of the Privacy Act of 1974. ICE may also request and receive information from other federal agencies pursuant to section (b)(7) of the Privacy Act of 1974. Agents and officers may upload documents received or manually enter any pertinent information from these sources into ICM.

IT system interconnections

ICM also contains data collected via system-to-system connections with other IT systems, including both DHS and external systems.[14] ICM users may search ICE and external databases, as detailed below, from within the ICM application and, depending upon the system, either directly import the data into structured forms or manually copy and paste or type the data into Subject Records or narrative documents:

[14] With the exception of TLS and FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS), to which the ICM application has direct connections, all connections to other systems are facilitated by the Interface Hub.

- ICE EID – ICM users may search and retrieve data on individuals (those arrested by HSI or ERO) from EID from within ICM. This is most commonly done when users are creating a person Subject Record, but may be done for other reasons related to an investigation. HSI agents and ERO officers use the EID Arrest Guide for Law Enforcement (EAGLE) module in EID to record booking information when they make arrests in the field. When a booking record is created in EAGLE, an event number is generated. An ICM user may place that number into the structured "event number" from within ICM when creating a Subject Record and select EAGLE as a search source. If the record is found, ICM pulls all information contained in EID collected via EAGLE on that individual into the appropriate structured fields (e.g., name, address) in the Subject Record. ICM users are instructed during training that this is the preferred method for creating Subject Records on individuals who have been arrested, because it ensures data between the two systems is consistent and minimizes data input errors.
- ICE FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS)[15] – ICM users are able to search FALCON-DARTTS from within the ICM application for Financial Crimes Enforcement Network (FinCEN) data and manually enter it into Subject Records and case documents. This includes the following types of FinCEN reports: Currency and Monetary Instrument Reports; Currency Transaction Reports; Suspicious Activity Reports; Reports Relating to Coins and Currency Received in Nonfinancial Trade or Business; and Reports of Foreign Bank and Financial Accounts.[16]
- ICE Student and Exchange Visitor Information System[17] (SEVIS) – SEVIS includes biographic and immigration status data related to individuals who are temporarily admitted to the United States as students or exchange visitors. ICM users may search SEVIS from within ICM and either directly import or manually copy SEVIS data into a case record. This is most commonly done when creating a Person Subject Record, but may be done for any investigative purpose.
- CBP TECS Platform – ICM users may query the CBP TECS Platform for information related to any person associated with a case. The CBP TECS Platform is expected to have the same type of information that CBP maintains in the TECS system today, including Subject Records, border crossing, and inspection records. This query process may be done, for example, when an ICM user is creating a person Subject Record or

[15] DHS/ICE/PIA-038 – FALCON Data Analysis & Research for Trade Transparency System (FALCON-DARTTS): https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falcondartts_january2014_0.pdf
[16] *See* the FALCON-DARTTS PIA for more detail about the information each of the listed reports contains.
[17] DHS/ICE/PIA-001(a) Student and Exchange Visitor Information System (SEVIS): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis.pdf.

looking for additional information on a person for whom the user has already created a record. If CBP has a record on the individual and ICM does not, the ICM user may create a Subject Record directly from the CBP record. If ICM already has a Subject Record pertaining to the individual, the user may either enhance the existing Subject Record with CBP's information or create a sub-record that is linked to the ICM master Subject Record.[18]

- CBP's Seized Assets and Cases Tracking System (SEACATS)[19] – ICM users may query SEACATS from within ICM to obtain records of seizures of contraband.[20] Typically, this occurs when a user is creating a seizure report within a case. The user can directly import the data from SEACATS into the seizure report. Information from SEACATS may also be manually input into other case documents, such as ROIs or arrest reports.

- CBP Automated Targeting System (ATS)[21] – ATS collects information from a wide variety of sources for the purpose of identifying potential threats to the border and public safety. These sources include, but are not limited to, other DHS systems and commercial carriers in the form of a Passenger Name Record. ICM users may query ATS from within ICM for information on passengers, vehicle, or aircraft border crossings, secondary inspection logs, visa and passport data, and other information relevant to investigations and manually copy any pertinent data into Subject Records or case documents.

- Department of Justice Federal Bureau of Investigation's National Crime Information Center (NCIC) System[22] – ICM users may query the NCIC system from within ICM via ICE's existing connection to NCIC.[23] This connection is housed within ICE's Alien Criminal Response Information System,[24] which is managed by ICE ERO's Law

[18] The CBP TECS Platform will replace the Legacy TECS system. For a period of time, ICM will exchange the data described above with Legacy TECS as well until the CBP TECS Platform is fully operational and Legacy TECS is retired.
[19] The DHS/ICE-008 Search Arrest and Seizure Records SORN was last published December 9, 2008 (73 Fed. Reg. 74732) and the DHS/CBP-013 Seized Assets and Case Tracking System SORN was last published December 19, 2008 (73 Fed. Red. 77764).
[20] These records may originate with CBP as a result of seizures made by that agency at the border or may originate with ICE HSI agents. CBP manages the physical assets seized by HSI agents and typically documents those seizures for HSI in SEACATS. HSI agents also have direct user access to SEACATS and may document their own seizures when circumstances warrant doing so.
[21] DHS/CBP/PIA-006 Customs and Border Protection Automated Targeting System (ATS): https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats_updated_fr_0.pdf
[22] FBI-001, National Crime Information Center (NCIC) (September, 28, 1999, 64 FR 52343): https://www.fbi.gov/foia/privacy-act/64-fr-52343
[23] Federal agencies are generally permitted only one direct portal into NCIC.
[24] DHS/ICE/PIA-020 Alien Criminal Response Information Management System (ACRIMe): https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_acrime.pdf

Enforcement Services Center. NCIC, owned by the FBI's Criminal Justice Information Services Division, contains information on criminal targets, immigration violators, and stolen articles. It also contains data from Nlets (not an acronym), a non-profit organization owned by the 50 states that facilitates the exchange amongst federal, state, and local law enforcement partners of law enforcement, criminal justice, and public safety-related information. The data that ICM users may collect from NCIC includes but is not limited to warrants that are input by other law enforcement agencies, terrorist watchlist records, state and federal criminal history reports, and reports of missing persons.

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

Yes. ICM users may collect and enter commercially available data and public (i.e., open source) information into ICM on an *ad hoc* basis; however, users may not query commercial or public sources from within ICM, and ICM does not ingest data directly from these sources. Some ICM users have access to commercial or public sources as part of their official duties and may manually incorporate this information into reports and/or Subject Records contained in ICM if the user determines that the information is relevant to the investigation. Such incorporation is at the discretion of the user and is not the result of an automated collection process. In some cases screen-shots of information from the Internet may be captured and uploaded to the ICM case file.[25]

ICM users may directly or indirectly (via a commercial data provider) access public information on the Internet, including social media websites, during the course of investigations and incorporate that information into case documents. In the case of undercover operations, information may be collected that is not publicly available but can only be viewed by those who have connected or "friended" the individual on social media sites, or who have otherwise been given special access to a restricted site.[26] These instances are limited to agents who are engaged in authorized undercover operations during the course of a criminal investigation.

ICE personnel use data from commercial sources and publicly available data to verify information contained in ICM; for example, to verify targets' former and current places of residence, former and current cohabitants, and/or to identify personal property owned by these targets. Furthermore, commercial or publicly available data may be used to enhance existing case information, such as providing additional identifying details (e.g., DOB), or public record data (e.g., civil litigations, criminal history, incorporation records).

[25] In collecting and retaining publicly available information from online and commercial sources, ICE operates in accordance with established DHS and ICE policies pertaining to the use of online information.
[26] For example, an undercover agent who is working a child pornography case may obtain access to a file-sharing site from the site administrator once the agent has established credibility with that administrator.

2.4 Discuss how accuracy of the data is ensured.

Data Integrity Controls During the Data Migration Process

All ICE-owned records were migrated into ICM from TECS prior to the launch of ICM, first into a temporary Target database, and then into both ICM and the HSI Data Warehouse. The IT team responsible for the migration conducted data verification at all phases of the migration – during staging of the data in TECS, once the data was migrated into the Target database, and when the data was finally migrated into ICM and the HSI Data Warehouse. Data verification practices included record counts, log verifications, statistics/queries based on over 160 unique criteria provided by HSI, and spot checks. The Target database was refreshed with production data multiple times after the initial migration, with verification taking place after each refresh.

Beginning in the fall of 2015, a special team of HSI personnel supporting the ICM development effort began validating legacy TECS records after they had been migrated into the ICM environment. HSI and the data migration team conducted validation activities with roughly 40 HSI representatives from ten offices, including field agents and supervisors. Additionally, during a User Acceptance Testing session, a handful of HSI representatives conducted spot-check data validation. At the time of launch, the data migration team had not received any reports of inaccurate or missing data.

Operational Data Quality Controls – Case Deconfliction

ICM's built-in deconfliction processes help to connect investigative efforts that are related but in a way that is unknown to the case agents. They also help to ensure data quality not only by identifying and resolving potentially conflicting information among investigations, but also by ensuring that the system contains the most complete information available to ICE on a particular target or other subject of interest. ICE personnel are required to query ICM prior to creating a new case file or Subject Record in ICM. If a case file or Subject Record does not already exist in the system for the intended subject of the new record, the user may create a new case file and/or Subject Record. If there is an existing case file, the system will provide the user with the name and phone number of the agent or officer who has an open case already in progress. The two can confer to determine if there is a reason to open a collateral (i.e., related) case under the existing investigation, or open a completely unique investigation. This ensures that two agents within ICE do not have two concurrent cases on the same individual or organization for the same criminal activity. If there is an existing Subject Record, the user is only able to create sub-records and link the master record to their own cases, Subject Records, and/or case documents. The system also alerts record owners each time another user, with the exception of OPR users, queries or views their Subject Records. This structure helps to ensure consistency and identity resolution in the information that ICE maintains about its investigative targets and other individuals.

Cases involving the same person or organization with multiple violations could also be combined, resulting in all information pertaining to a given subject being linked, documented, and displayed in one view. For instance, if an individual is suspected of both drug and alien smuggling, that individual's records may be combined into one case with multiple violations of law. This case-by-case determination is made based on an analysis by all law enforcement stakeholders (e.g., agents/officers, prosecuting attorneys) of whether combining the cases will ultimately improve the results of an investigation and/or prosecution.

Other Operational Data Quality Controls

ICM data: As a primary safeguard, ICM users are required to undergo intensive training in the use of the system before they are given access. Once they are able to use the system, they have ongoing access to a training "sandbox" that replicates the functionality of the system using "dummy" (synthetic) data.

As a matter of ICE policy, ICM users are required to take steps to ensure that data entered into the system meets the highest possible data quality standards and to correct inaccurate data. This is a critical need for the integrity of investigations, and also serves to promote individual privacy interests. To this end, during investigations HSI special agents and support personnel compare new information with information already in the system and external investigative case files before entering the information in ICM. This comparison process allows the user to recognize and resolve conflicting and inaccurate information before such information is memorialized in the system. Users are also instructed that the preferred method of creating certain types of Subject Records is by importing data from another system after verifying the accuracy of the data (e.g., SEACATS for Subject Records pertaining to seized assets and EID for Person Subject Records when the individuals have a booking record in EAGLE). This preference ensures data quality both within ICM and across DHS systems.

Additionally, the system allows users to regulate each other's data quality. For example, if two users have identified the same individual in Person Subject Records, ICM allows users to compare the information and resolve discrepancies to ensure data accuracy. HSI special agents and support personnel also maintain original source information in a hard copy investigative case file, separately from ICM. Hard copy files, which contain proper data classification markings, are maintained in locked cabinets in a secured building with access limited to those who have a need to know. As exists currently with TECS, hard copy case files contain, in part, printouts of electronic information (e.g., ROIs, Subject Records, and arrest/seizure reports) contained in the system. These hard copy files also contain information derived from other sources including court documents, reports from other agencies, investigative notes, and other documents that are not maintained in an electronic system. Thus, ICM information can always be checked against the original source data to ensure accuracy. ICM allows record owners to modify their own Subject Records to correct inaccurate data.

Finally, ICE policy requires that Subject Records and case documents must be reviewed and approved by a supervisor prior to being considered available for use in an investigation, and controls to implement this policy are built into the system. For example, ROIs created by ICM users are first created as drafts; the drafts must be approved by a supervisor before they are considered final and available for viewing by other ICM users. In contrast, Subject Records created by ICM users are immediately viewable to other ICE users because of the need to deconflict them (and because of officer safety concerns), but they are flagged to indicate they are pending until a supervisor reviews and approves them. Copies of ICM records are not placed in the HSI Data Warehouse until they are approved.

TLS/Pen-Link data: Each record in TLS is checked using an automated data quality filtration process to ensure the quality of the data, specifically that duplicate or improperly formatted data is not loaded into the TLS system. As a best practice, agents who create subscriber records are expected and trained to ensure the accuracy of the data in those records by comparing it against the authoritative source upon which it is based.

Finally, ICE has a dedicated data quality unit whose mission is to work with special agents and support personnel in the field to ensure that ICE systems in general, and ICM in particular, meet data quality standards. OPR also maintains a unit responsible for assessing organization performance, the efficiency and effectiveness of both office and management operations, and compliance with the policies and procedures of programs and offices with ICE. This unit will use ICM to conduct its inspection mission to ensure the accuracy, timeliness, and completeness of case management policy requirements.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information will not be accurate, complete, or timely.

Mitigation: This risk is partially mitigated by the immediate availability of new and updated Subject Records in ICM for purposes of deconfliction and to ensure that all users have the most complete information available at any given time. These new and updated records are flagged as preliminary, however, until a supervisor approves their addition to the case file. All substantive ICM data that has been approved is loaded into the HSI Data Warehouse once every 24 hours to ensure that the information relied upon for sharing and reporting is as timely as possible.

ICM users are also instructed to verify their own data prior to submitting records for approval, and to contact other record owners to resolve any discrepancies they identify when viewing the records of other ICM users. Data in the system may be checked against hard copy investigative case files and against other separately maintained original source data (e.g., evidence, original call detail records) to ensure accuracy. ICE promotes accuracy and integrity when using commercial or publicly available data from multiple sources by using credible, industry-wide

sources to increase the probability of identifying valid, relevant information. Also, users are trained to validate all commercial or publicly available data against authoritative sources, such as other federal records, before considering that information to be credible.

Privacy Risk: Because data is both imported[27] and uploaded/input on an *ad hoc* basis from multiple systems and sources, there is a risk that ICM may collect more information than is necessary to meet the needs of a given investigation.

Mitigation: This risk is mitigated in multiple ways. First, while ICM does have system interfaces that allow it to collect information from a broad array of other Government databases, it does not perform these searches by default. The ICM search function defaults to an ICM-only query and users must affirmatively select other systems to query as needed. Second, personnel are also trained to manually collect only data that is relevant for developing a viable case and that supports the investigative process. The information that goes into ICM is curated by trained investigators. They collect and retain information that appears to have probative value at the time that it is collected. It is normal in investigations that information considered probative at one point in time may later be determined to be irrelevant to a case. However, it is also possible that information considered probative in a case may ultimately be exculpatory in either the immediate case or a linked case. Finally, supervisory review and oversight helps to ensure that the data in the system is consistent with the purpose of the program.

Privacy Risk: Because ICE may create Subject Records on individuals who are not targets of investigations, there is a risk that these individuals may be mischaracterized as, or misunderstood to be targets. Among other concerns, this may cause individuals to experience difficulties at ports of entry where CBP uses Subject Records in screening.

Mitigation: This risk is mitigated in three ways: 1) The system allows personnel to amend the Subject Records they create to ensure they are accurate and, where necessary, annotated with appropriate contextual information. Investigators are trained on the proper use of the system and are also trained and expected to ensure their case files are accurate and up to date, as inaccurate information about subjects is detrimental to their investigations. Correcting Subject Records is especially important when an individual who is initially suspected as a target is later determined to be a victim or witness; for example, in the case of identity theft, when a target uses a victim's identity in the commission of a crime. In such a case, ICM users annotate the Subject Record in the comments section to note that the individual was first thought to be a target but has now been confirmed as a victim. Further, ICM users are trained to fully review all records when relying on the information therein for investigative purposes. In addition to ensuring they are using all information at their disposal when developing theories of a case, this also enables user to identify

[27] Note that "import" does not mean bulk ingest from other source systems. ICE users of ICM may directly import data from other systems into structured forms or manually copy and paste or type the data into Subject Records or narrative documents.

any inconsistencies in information that might indicate an inaccuracy in the records and take quick action to correct the records. Finally, as previously noted, supervisors must review and approve Subject Records and ROIs before they are considered final. This serves as another set of eyes that may detect inaccuracies. 2) ICM users are able to unlink one Subject Record from another. For example, the Subject Record of a witness initially thought to be a criminal associate of a target and linked to the Subject Record of that target may be unlinked so the witness's record no longer appears in search results for the target. 3) Because ICM pushes Subject Records to the CBP TECS Platform on a continual basis, when inaccuracies are corrected in ICM Subject Records and/or records are annotated, they will be available to CBP soon after. However, individuals may still experience difficulties at ports of entry as a result of lookout records. When this occurs, those individuals may submit complaints to the DHS Traveler Redress and Inquiry Program (DHS TRIP). If DHS TRIP determines that information in an ICE Subject Record is the reason a traveler is experiencing difficulties, ICE will review and correct the record, if warranted.

Privacy Risk: ICE's surveillance activities, including video and LPR technology, create a risk of overcollection of information that is not related to a law enforcement action.

Mitigation: While additional data that may not be relevant to an investigation can initially be captured as a result of any surveillance activities, ICE law enforcement personnel are trained to extract and load into ICM only the data that has probative value. In accordance with evidence handling policies, ICE keeps copies of video footage and audio recordings outside of the system as a safeguard, as not doing so creates a risk of destroying potentially relevant – including exculpatory – information. In the case of LPR technology, the data described in this PIA and retained in ICM is obtained directly by ICE using ICE-owned cameras, or by other law enforcement agencies, typically from targeted, strategic locations, and provided only to ICE and other law enforcement agencies in support of investigative and enforcement activities. Any images that are not related to a particular investigation are not placed in ICM or otherwise retained by ICE.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

HSI and ERO personnel use the information in ICM to document and inform their criminal investigative activities and to support the criminal prosecutions arising from those investigations. ERO also uses ICM data to inform its civil cases.

Subject Records and case documents: Subject Records and case documents such as ROIs and incident reports are used to document additional investigative information, draw connections

between subjects and cases, and inform subsequent case activities. Biographic data in Person Subject Records is used for case and identity deconfliction purposes. Case deconfliction is when the record is used to ensure a case agent knows there is some existing identity information and possibly an investigation on an individual for whom they are creating a Person Subject Record. Identity deconfliction is when the record is used to ensure one individual does not have two Subject Records. Incident reports, including arrest and seizure records, as well as case documents containing photographs or copies of evidence, help ICE maintain organized and complete investigative files and are ultimately used to support the criminal prosecutions of its cases by the U.S. Department of Justice or state/local prosecutors. ICE Subject Records are also used by CBP as "lookout" records to assist CBP personnel in conducting screening at exit and entry at U.S. borders. Other users/uses of these records include:

- By HSI, via the FALCON-SA system, to conduct search and analysis of data to support various HSI law enforcement efforts, including the production of law enforcement intelligence products, providing lead information for investigative inquiry and follow-up, assisting in the conduct of ICE criminal and administrative investigations, assisting in the disruption of terrorist or other criminal activity, and discovering previously unknown connections among existing ICE investigations.
- By ICE ERO, via ICM, to support and inform its criminal and civil law enforcement activities.

OPR uses Subject Records and case documents in both the ICM system and the HSI Data Warehouse, as well as audit log files, to support and inform its investigations into allegations of employee misconduct. OPR may also use data from ICM in other ways to support its oversight responsibilities. OPR is responsible for assessing organizational performance, the efficiency and effectiveness of both office and management operations, and compliance to policies and procedures of programs and offices within ICE. For example, OPR may query an ROI in ICM during the course of an audit to determine whether it was created within the timeframe specified in policy. EIRU and supervisors with direct access to the HSI Data Warehouse also use these records to prepare reports on case management related metrics and support data analytics. For example, the data may be analyzed to determine law enforcement trends and thus inform more effective allocation of resources.

Finally, external law enforcement agencies use ICM data in support of their investigations and/or agency missions, as described more fully in section 6.0. External agencies may receive this information either via a connection between their systems and the HSI Data Warehouse pursuant to established formal agreements, or as a result of routine use disclosures, as provided for in section (b)(3) of the Privacy Act of 1974.

TLS/Pen-Link data: ICE uses the telecommunications data contained in the TLS application within ICM in support of its investigative activities. It is included in Subject Records,

ROIs, and/or uploaded in spreadsheets that are linked to a case. The data is used primarily to identify connections between targets and criminal associates in support of investigations into criminal organizations. ICM users may search and analyze TLS data (which is stored within ICM) via a dedicated tab in the ICM application that is available when a user is viewing a case record. Information returned on the search, such as subscriber and/or call data information, cannot be directly imported into an ICM record. Users may elect to copy and paste or otherwise manually enter relevant TLS data into comment fields in Subject Records or narrative case documents, such as ROIs.

Location tracking device and LPR data: The location tracking device data and LPR data contained in ICM are also used in support of ICE's criminal investigative activities. The data is included in Subject Records and ROIs and, in the case of pictures or other external documents, may be uploaded to ICM case files. It is used to track patterns of movement, indicate the location of a target at a specific time, and inform immediate action (e.g., to support apprehension of a target) as needed.

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.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to or inappropriate use or disclosure of information contained in ICM or the HSI Data Warehouse. The significance of this risk is enhanced due to ICM's law enforcement purpose and the nature of the information about individuals that is contained in the system.

Mitigation: This risk is mitigated by user training, controls on access to ICM and the HSI Data Warehouse, operational oversight and information security controls.

Training and access controls: Annual Information Assurance Awareness Training is mandatory for all ICE personnel and ICM users also must complete mandatory ICM-specific training, including privacy training, before they gain access to the system. This training has a significant portion dedicated to privacy. ICM users have role-based permissions to ICM and role-based training is required. Roles are defined by job position, duty, and office assignment, and users

are granted the lowest level of privileges necessary to perform their job-related responsibilities. If an ICM user requires access to NCIC data (e.g. criminal history, warrants), they are also required to be NCIC-certified, which demonstrates that they know the special rules for handling criminal justice information in that system. If an ICM user's NCIC certification has expired, they will still be allowed into ICM but will not be able to run NCIC transactions until their NCIC certification is up-to-date. Access to the HSI Data Warehouse is limited to EIRU, supervisors with a job-related need for access, and OPR. Finally, when determined appropriate by record owners and their supervisors, the originators of cases or records in ICM may limit the access of other ICM users to that information, with the caveat that a user may not limit his or her supervisor's access to information.

Operational oversight and information security controls: Before a user logs in, a warning banner is displayed in ICM advising the user that he or she has no expectation of privacy with respect to any actions taken while in the system. ICM and the HSI Data Warehouse have robust auditing features to help identify and support accountability for user misconduct. The audit logs capture user activity including, but not limited to, uploading records or data, extracting information from the system, resolving entities, searches, and viewing records. OPR has access to these audit logs, and disciplinary actions for violations of ICE policies and rules of behavior regarding the system are taken when warranted.

ICM users will receive an email and a notification message in their notification queue when another individual has queried their record, document, and/or case in the system, the search criteria he or she used, and whether the information was displayed. (The exception is when an OPR user queries a record.) This allows users to monitor when other users access their records, including ROIs and Subject Records, and inquire as to why another user has conducted a particular query or viewed a record. This can reveal misconduct on the part of users who may be inappropriately browsing the system, but also serves as a deterrent as users know it is likely inappropriate activity will be challenged or reported. Query notifications bring a transparency to the system that may also reduce duplication of effort. Users are trained to report suspected misuse of ICM or misconduct associated with ICM use to management and/or file a report directly with OPR.

Finally, ICM data may be manually shared with agencies outside of ICE in accordance with formalized agreements (e.g., a Memorandum of Understanding) or pursuant to *ad hoc* requests that conform with the requirements the Privacy Act of 1974. Formalized agreements must be reviewed and approved by various oversight offices within ICE and DHS. This helps to ensure the sharing is supported by legal authorities and consistent with the purposes for which the information was collected.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

Notice of the existence, contents, and uses of ICM and TLS are provided by the publication of this PIA and by the ICE External Investigations SORN (DHS/ICE-009[28]). Because ICM and TLS are law enforcement systems that collect and maintain 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 input into the system. When ICE agents and officers interact with individuals in connection with an investigation, however, those individuals are generally aware that their information will be recorded and stored. ICE agents and officers take biographical information from the individuals with whom they interact and write it in field notes in plain view of those individuals. They also typically inform victims and witnesses that the information they provide 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, notices on the relevant forms that generally state that the 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?

In most cases, because of the law enforcement purposes for which the information is collected and used, opportunities to decline or opt out may be limited or nonexistent. ICM users may enter data during the course of a law enforcement activity or in support of other DHS proceedings, and it is the nature of the proceeding and the rights afforded to an individual by law that will determine the ability of a person to exercise the right to decline to provide information. For instance, in the case of an administrative or criminal arrest, the individual is advised of his or her right to refuse to provide information pursuant to the Fifth Amendment. By providing information after receiving such a warning, the individual consents to any lawful use of the information. The only means by which the individual can withhold consent to any particular use of information is by refusing to provide the information.

[28] DHS/ICE-009 External Investigations SORN (January 5, 2010, 75 Fed. Reg. 404).

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware their information may be contained within ICM or TLS or understand how ICE uses the information collected about them.

Mitigation: Individuals who are questioned directly by ICE personnel have notice by virtue of the encounter itself that ICE is conducting an investigation. Although there is a potential risk that a language barrier may cause communication issues when ICE encounters an individual, attempts are normally made to communicate with individuals in their native language or through an interpreter. In addition, the United States has agreements with some nations that require notification of the foreign government's consular office when a national of that country has been arrested, and in other cases the individual always has the right to request consular notification and assistance. The engagement of the consular officials can assist individuals from other nations in understanding the criminal proceedings against them, obtaining legal counsel, and obtaining other resources that may be of use.

There is a countervailing risk that arises when individuals are notified that information is being collected about them by ICE for law enforcement purposes. Such notification may be the proximate cause of compromising an investigation, especially if the individual decides to flee, or destroy or conceal evidence as a result of this notice. This risk directly affects the ability of ICE to perform its mission. Furthermore, release of such information could pose officer safety issues for law enforcement personnel. In such cases, ICE may intentionally withhold notification to the individual until he or she is arrested or indicted.

In addition to the notice described above, some service providers who are required to provide subscriber information to ICE pursuant to a subpoena will, in certain instances, inform subscribers that they have provided information to ICE. Also, public notice is provided through this PIA and the associated SORN that inform the public how ICE uses the information it collects in criminal and civil investigations.

Section 5.0 Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Under the proposed records retention schedule for ICM, ICE intends to request NARA approval to retain ICM records for 20 years from the end of the fiscal year in which the case was closed. Cases deemed significant pursuant to criteria detailed in the proposed records schedule because they are of historical interest will be retained permanently. This retention schedule is

consistent with the proposed DHS Enterprise Schedule for Investigative Records. After the 20-year period, the information would be destroyed or, if deemed necessary, retained further under a reset retention schedule. The 20-year period provides reasonable assurance that the records of individuals who may be encountered multiple times over a prolonged period of time will be linked.

All ICM records will be treated as permanent records until a records retention schedule is approved. ICE intends to request the same retention schedule for TLS records, as they are also investigative records, and will treat TLS records as permanent until a records retention schedule is approved.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: The proposed 20 year retention period for ICM and TLS records is consistent with the retention schedules for other investigative records within DHS. This retention period will support the effective enforcement of U.S. immigration laws by ensuring that information pertaining to individuals who are encountered repeatedly over a span of time can be linked. Closed cases can contain information that may be relevant to a new or existing ongoing case and need to be readily searchable and accessible for at least a period of time.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government and private sector entities.

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.

Consistent with federal law and DHS policy, information from ICM is shared outside of DHS with other agencies that demonstrate a need to know the information for the performance of their missions. Information is shared pursuant to Memoranda of Understanding or through sharing between ICE personnel and other agency personnel by other means; for example, among those law enforcement officials assigned to a joint investigation or with prosecuting agencies. ICM data will be shared if doing so will further law enforcement efforts conducted by ICE or its law enforcement partners, and provided that disclosure is consistent with applicable law and agency policies. ICM information will be shared with federal, state, tribal, local and foreign law enforcement agencies,

as well as relevant law enforcement fusion centers, FBI Joint Terrorism Task Forces, and international organizations such as INTERPOL. All external sharing of ICM information will be documented using applicable disclosure procedures per DHS policy and applicable statute. This sharing is done manually by ICE personnel and not via system-to-system connections.

TLS data is routinely shared in bulk with the Drug Enforcement Administration (DEA) to support its investigations, and for the following purposes: officer safety, deconfliction and coordination with other federal investigations, to contribute to federal analytics of law enforcement investigations in certain key areas, and to obtain the results of those analyses to further the ICE criminal investigation. DEA is bound by the same statutory information protection requirements to which ICE is bound to adhere.

ICM Subject Records and the investigation case number associated with a Person Subject Record will be shared with partners via the Law Enforcement Information Sharing Service (LEIS Service), which is operated by ICE on behalf of DHS.[29] The LEIS Service provides access to DHS information to external federal, state, local, tribal and international law enforcement agency partners. These partners use the LEIS Service as a sharing service to access filtered law enforcement information from various DHS systems, including Legacy TECS and now ICM. These partners access the data via federal, state, local, tribal, regional, or international information sharing services to which they belong and through which the queries to the LEIS Service are made. Sensitive but unclassified DHS law enforcement information is provided in an automated response along with contact information for relevant DHS law enforcement officials. No unstructured text contained in narrative sections of Subject Records or ICM case documents, such as ROIs, is shared through the LEIS Service. Only selected fields from these records can be shared in response to queries. Additional information about how the LEIS Service operates and the data shared that originates from ICM can be found in the LEIS Service PIA.

ICE also discloses limited information from ICM to obtain information from sources such as witnesses, recipients of subpoenas, and sources of commercial and public data. Information is disclosed in these situations where personnel conducting investigations believe that the parties to whom they are making the disclosure have relevant information. ICE personnel disclose only the information necessary to receive the information they need.

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

[29] See DHS/ICE/PIA-004(a) ICE Pattern Analysis and Information Collection (ICEPIC), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-pic-january2008.pdf. A separate PIA documenting the LEIS Service will be published later in 2016 based on the retirement of the ICEPIC system which formerly housed the Service, as well as updating the source of the Subject Records and other case data from TECS to ICM.

The sharing of PII with law enforcement agencies outside of the Department is compatible with the original purpose for collection, namely to conduct criminal law enforcement investigations and other enforcement activities, to uphold and enforce the law, and to ensure public safety. All external sharing falls within the scope of applicable law, including the published routine uses in the DHS/ICE-009 External Investigations SORN.

6.3 Does the project place limitations on re-dissemination?

Federal agencies that receive ICM information are subject to the Privacy Act and, as such, may not re-disclose information without clear authority to do so. Additionally, ICM information is shared with other agencies pursuant to information sharing agreements, those agreements include provisions for appropriate and adequate safeguarding of sensitive information. Commercial data providers with whom ICE shares limited information contained in its queries to their systems are prohibited under terms of their contracts from re-disseminating ICE information. They are also required to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information, and notify ICE if they become aware of any breach of security of interconnected systems or potential or confirmed unauthorized use or disclosure of personal information.

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

ICM users are required to complete and retain DHS Form 191, Privacy Act Disclosure Record, when making an external disclosure. Currently, ICM users complete a paper form and maintain it in their hard copy case files. In a future release, ICM users will be able to complete this form electronically from within the system and store it in the ICM case file.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that data will be shared with external parties lacking a need to know, and that external sharing will not be properly recorded as required by the Privacy Act.

Mitigation: ICM users are required by law and policy to share information with only those external partners who have a demonstrated law enforcement, intelligence, or national security need to know. This requirement is in keeping with the law enforcement purpose of the ICM system, the TLS subsystem, and ICE location tracking projects and technologies. As noted above, they are also required to complete DHS Form 191, Privacy Act Disclosure Record, when they make external disclosures. Supervisors routinely review their subordinates' case files and inspect these forms as part of their review. This risk is also mitigated by the fact that only ICE authorized users have direct user access to the system. ICM and its components use SSO with PIV-card

authentication, which reduces the risk of unauthorized access and, therefore, unauthorized sharing, and also enables tracking and auditing of user activity.

Further, ICE employees and contractors are trained on the appropriate sharing of PII and to contact the ICE Privacy Office if they are not certain whether information sharing is appropriate. ICM users receive additional privacy training specific to their use of ICM that covers the rules for disclosures to parties outside of DHS. Finally, commercial data providers are restricted from re-disclosing ICE information (e.g., minimal subject-related data contained in queries) pursuant to the terms of their contracts with ICE.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals seeking notification of and access to any of the records covered by this PIA may submit a request in writing to the ICE Freedom of Information Act (FOIA) officer by mail or facsimile:

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/

All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target 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 the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

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

Individuals seeking to correct records contained in this system of records, or seeking to contest its content, may submit a request in writing to the ICE Privacy and Records Office by mail:

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

All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension.

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 Freedom of Information and Privacy Act requests. No individual notification of procedures for correcting ICM records is currently provided, however. ICM contains investigatory material compiled for law enforcement purposes and is exempt from the amendment provisions of the Privacy Act. Notification to individuals that they are or have been the target of a law enforcement investigation could undermine the law enforcement mission of ICE.

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: Because ICM and TLS contain data maintained for a law enforcement purpose, individuals' rights to be notified of the existence or non-existence of data about them, and to direct how that data may be used by ICE, are 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 associated SORN provides general notice about ICE's collection of information and the uses to which that information is put. In addition, in exempting its investigative systems from access and amendment under the Privacy Act, ICE has indicated that the exemptions will be applied 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

The following questions are intended to describe technical and policy based safeguards and security measures.

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

ICM ensures information is used in accordance with the stated practices in this PIA through access controls, query notification, auditing, and supervisory review. ICM will actively prevent access to information for which a user lacks authorization, as defined by users' need to know and job responsibilities. The user who created a case or record in ICM may limit the access by others to that information, with the exception of the originator's supervisor. Users are required to complete system-specific, role-based training before being granted an account.

Query notifications provide another accountability measure. ICM users receive a notification whenever another user has viewed a document of theirs in the system. Using this functionality, users can "police" their records, including ROIs and Subject Records, by having notice and the ability to inquire as to why another user has conducted a particular query. Query notifications bring a transparency to the system that discourages unauthorized browsing for information. If a user suspects or has reason to believe their records have been misused in any fashion, the user can report the suspected misconduct to OPR for further investigation.

In addition to access controls and query notification to the users, there is a very detailed set of auditing requirements that are tracked and saved in audit logs for viewing later by OPR if allegations of misuse are made against a user. ICM keeps copies of audit and log file data in a separate data repository in which it will be retained for 7 years to ensure ICE will be able to track and investigate misconduct and misuse of the system. The audit logs account for ICM transactions,

as well as information sharing activity that occurs through the Interface Hub and queries of the HSI Data Warehouse. Misuse of the system may subject a user to criminal and civil penalties, as well as discipline in accordance with the ICE Table of Offenses and Penalties, up to and including removal. OPR users who query ICM and the HSI Data Warehouse have their activity tracked in the audit logs, although their queries and viewing of ICM case records do not trigger notifications to the case agent for that investigation. This is to preserve the integrity and confidentiality of any OPR investigation that may be ongoing.

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

In order to gain and maintain access to the system, ICM users must take and pass an ICM user training course that includes in-depth privacy training. Upon gaining access to the system, a user will be required to recertify his or her ICM training every year. An automated "guard" will be implemented wherein a user's access will immediately be denied by the system if he or she has not successfully and timely completed the training. Additionally, all ICE employees are required to take annual DHS privacy training and ICE Information Assurance Awareness 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?

Only ICE personnel whose official duties necessitate access to ICM and TLS data covered by this PIA will be granted access. ICE management oversees and approves the assignment of user accounts to ICE personnel. An ICM administrator establishes ICM user accounts and updates user role-based permissions, as needed. Access roles are assigned by a supervisor based on the user's job responsibilities, and implemented by an ICM administrator. Access roles are reviewed regularly to ensure that users have the appropriate level of access. Individuals who no longer require access are removed from the access list.

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 Systems Security Officer, the ICE Privacy and Records Office, the Office of the Principal Legal Advisor, key program stakeholders, and the Program Manager and

then sent to DHS for formal review. ICE Memoranda of Understanding (MOUs) clearly articulate who will be accessing the shared information and how it will be used. If the terms of existing MOUs are changed, addendums will be established and reviewed in the same manner as described above.

Responsible Officials

Lyn Rahilly, Privacy Officer
U.S. Immigration & Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security