U.S. Immigration and Customs Enforcement

Immigration and Customs Enforcement (ICE) TECS Investigative Case Management (ICM) Statement of Objectives

U.S. ICE Office of the Chief Information Officer (OCIO) *and* Homeland Security Investigations (HSI)

May 1, 2014

Version 1.0

Homeland Security

Table of Contents

1. Purpose 3
2. Scope 3
3. Program Execution 3
4. Background 5
   4.1 Program Organization 6
   4.2 HSI Investigative Case Management Ecosystem View 7
5. Mission Capabilities for the ICM System 8
   5.1 Case Creation and Management 9
   5.2 Subject Record Management 9
   5.3 Data Migration of Existing Legacy TECS Subject Records 10
   5.4 Reports of Investigation 11
   5.5 Notifications 11
   5.6 Interfaces 12
   5.7 Flexible Linking of Cases, Documents, and Subject Records 12
   5.8 User Control of Access to Case-Related Information 12
   5.9 Transfers of Users, Cases, and Subject Records 13
   5.10 Searching Structured and Unstructured Data Across Document Types 13
   5.11 Agent Work Hours 14
6. Technical Capabilities for the ICM System 14
   6.1 Hosting Environments 14
   6.2 Key Performance Parameters and Maintainability 15
   6.3 Measures of Effectiveness 16
   6.4 User Provisioning 17
   6.5 Single Sign On 18
   6.6 Interfaces 18
   6.7 Data Migration 21
   6.8 ICE Data Warehouse 23
   6.9 Security and Privacy 23
   6.10 Data and Licensing 23
7. Implementation and Management 24
   7.1 Development, Test, and Deployment Approach 24
   7.2 Service Desk Support 25
   7.3 Maintenance Support 26
   7.4 Training Strategy 26
   7.5 Systems Engineering Lifecycle Documentation 26

7.6 Project Management 26
7.7 Key Personnel 27
8. Applicable Documentation 28
Appendix A - List of Acronyms 30

List of Figures

Figure 1: HSI Investigative Case Management Ecosystem View 8
Figure 2: CORE HSI Investigative Case Management Processes 9
Figure 3: Example of One-to-Many Relationships in HSI Subject Records 10
Figure 4. HSI User Provisioning for the ICM System 17

List of Tables

Table 1. ICE TECS Modernization Program Hosting Environments 14
Table 2. KPPs for the ICE TECS Modernization System 15
Table 3. ICE TECS Modernization System Interfaces 18
Table 4. Legacy TECS Data to be Migrated to the ICM System 21
Table 5. Tier 2 and 3 Performance Requirements 26

1. Purpose

The purpose of this Statement of Objectives (SOO) is to obtain a Commercial Off-the-Shelf[1] (COTS)-based, web-enabled Investigative Case Management (ICM) system. The ICM system will support the U.S. Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE)/Office of the Chief Information Officer (OCIO) and Homeland Security Investigations (HSI) mission, and will improve HSI's ability to investigate, manage, and report on law enforcement and intelligence activities.

Within the context of this solicitation, the ICM system is defined by the following criteria:

- Mature COTS-based, web-enabled solution that can achieve the aggressive schedule of delivering a production ready solution for formal integration testing within six months after contract award and that can be ready for initial operation no later than September 30, 2015
- System that can be configured or minimally customized to support the unique requirements of the ICE/HSI investigative law enforcement agency
- System that can integrate into the DHS and ICE enterprise infrastructure
- System that can interface with other specified systems that are internal and external to ICE and DHS via the ICE Interface Hub (see Figure 2 and Section 6.6)
- System that can interface with the ICE Data Warehouse (see Section 6.8).

2. Scope

The ICM system shall meet ICE/HSI requirements expressed at a high level in this SOO and in detail in Exhibit A. The Offeror shall provide the services and software to support the requirements outlined in this SOO in accordance with the Offeror's proposed Performance Work Statement (submitted by the Offeror in response to the request for proposal [RFP]), which will be incorporated into the contract at the time of contract award. The Government encourages Offerors to propose the most innovative, cost-effective solution and implementation methodology to achieve the desired objectives and results within the context of this solicitation. The Government's objective is to acquire an ICM system that:

- Creates and manages ICE/HSI investigative cases and documents
- Creates and manages HSI subject records that include information related to person, vessel, vehicle, aircraft, business, and other thing(s)
- Links subject records to reports of investigation (ROIs) and investigative cases
- Creates and manages lookout records shared with Custom and Border Protection (CBP)
- Performs investigative research via system interfaces both internal and external to ICE and DHS
- Creates and manages case statistics (i.e., arrests and seizures)
- Captures administrative data (such as agent work hours on cases)
- Generates reports on case-related data.

The Offeror shall implement, integrate, and test the ICM system in a Government facility and have the ability to provide operations and maintenance (O&M) support after Initial Operating Capability (IOC) and Full Operating Capability (FOC).

3. Program Execution

To successfully execute this SOO, the Offeror's team must integrate with the existing project teams supporting the ICE TECS Modernization program to promote seamless interoperability across the teams

[1] In the context of this procurement, the term "COTS system" means a previously developed and deployed system that requires minimum new development to meet ICE ICM system requirements.

while fostering transparency and information sharing. The other development teams have been focused on profiling and migrating the data from the legacy TECS environment into a target database, identifying data that needs to be integrated into the Offeror's solution, developing data services to support the interfaces with external systems, and developing documentation to support DHS system life cycle.

The Offeror shall propose a work schedule with timing and associated milestones required to achieve IOC in four consecutive defined time phases of work (i.e., Phases 1 – 4 below), the length of each phase will depend on an individual Offeror's proposed solution. The Offeror's work schedule shall be formatted according to the RFP's instructions to the Offeror regarding submission of a Contractor Work Breakdown Structure (CWBS).

The Offeror's work shall be executed in phases as follows.

Phase 0 (optional)-Proof of Concept: The Government has the option to award multiple contracts. The base period of each contract will consist of a two (2) month proof of concept period to support further functional and technical review of each Offeror's solution. During this period, the Offeror will build a proof-of-concept based on the operational flow described in Exhibit B. To minimize external dependencies, development and hosting shall occur at the Offeror's location during the 2 month base period. The functionality developed will need to be incorporated as part of the overall solution and not be developed as "throw away" code. At the conclusion of the base period, the Government will exercise Option Period 1 of the contract which is determined to offer the best chance of successful completion. No further options will be exercised on the other contracts.

The Government will use the proof of concept to validate and independently verify that the Offeror's solution can successfully navigate the operational flows referenced in Section 5 of this SOO and described in Exhibit B. The Government will also use the proof of concept to help verify that the Offeror can fulfill the ICM system Capabilities Matrix in the RFP as outlined by the Offeror in their response to the RFP. Any functionality developed in this time frame shall be incorporated as part of the overall solution. The proof of concept must demonstrate to the Government that the Offeror has a significant potential to successfully continue with configuration, development, and implementation of the ICM system solution.

Phase 1- Requirements Confirmation and Baseline Installation: The Offeror shall rapidly install their ICM system solution in the DHS/ICE development and test environment, or other environment proposed (see Section 6.1). The ICM system shall be configured and operable to the baseline level of functionality and technical capability representative of the COTS system solution installed at other customer facilities, as depicted in their past performance statements, and as documented in the Offeror's assessment of its baseline solution's capabilities (reported by the Offeror in the response to this RFP).

Phase 2-Baseline Gap Analysis: The Offeror shall perform a gap analysis of the baseline capabilities as installed in the first phase versus the required IOC capabilities. This gap analysis will be performed with the Offeror's resources and those of the ICE TECS Modernization program, for example the HSI users. Due to schedule constraints, the Offeror may propose overlapping Phase 1 and Phase 2 as deemed appropriate. However, Phase 3 should not commence until the Offeror develops a plan of action for resolving the gaps identified in this analysis and the Government approves said plan.

Phase 3-IOC Development and Configuration: The Offeror shall configure and develop the IOC capabilities as documented in the Baseline Gap Analysis and approved by the Government. This phase and the preceding phases 1 and 2 will end no later than six months after contract award and the end of this phase will constitute the "code freeze" milestone for IOC in which all ICM system development and configuration work is complete.

Phase 4-IOC Integration and Testing: This phase is targeted to end no later than six months after the completion of Phase 3. This phase of work will consist of extensive integration testing, system testing, performance testing, user acceptance testing, and stress testing of the ICM system solution with the ICE

interface hub, ICE Data Warehouse, and other ICE TECS Modernization system components required for the IOC as defined in Exhibit A. The Offeror shall participate in all levels of integration and testing as the overall ICE TECS Modernization system progresses to IOC. Specifically, the Offeror shall assist in analyzing problems discovered during all levels of integration and testing. The Offeror shall correct errors and shortfalls (example of shortfall is not meeting performance requirements) in the ICM system during all levels of integration and testing.

Note: Phases 1 through 4 constitute Option Period 1 of the contract and are included in the Firm Fixed Price portion of the CLIN structure.

FOC Capabilities. FOC capabilities and other system enhancements, if required, will be accomplished through optional System Enhancement CLINs for development, configuration, integration, and testing. This work will be accomplished on a Labor Hour (LH) basis as the exact scope of the FOC capabilities is undeterminable before completion of IOC. Some FOC capabilities may have been met in the offeror's base system.

Maintenance of the ICE System Solution. The Offeror shall provide their approach for maintenance of the ICM system solution. This approach shall include the Offeror's basic approach to ICM system bug fixes/patches, routine maintenance and upkeep of the ICM system solution, on licenses and upgrades on the Offeror supplied products associated with the ICM solution, and to upgrade frequency to the installed ICM system solution. The approach shall also stipulate the level of commitment of the Offeror in maintaining the ICM system solution in perpetuity or in transfer of the ICM system license to the Government and in training the Government or designees in this maintenance capacity.

Transition Out The Transition Out phase will provide the Government with a Transition Management Plan (TMP) 90 calendar days prior to the completion of the period of performance (POP). The Offeror shall provide their approach for supporting export of all ICE data in the ICM system in a format usable by, and approved by, the Government to a different product if desired by the Government. The technical activities included as part of the TMP shall consist of the following:

- Provide inventory and orderly transfer of all Government Furnished Equipment/Property (GFE/GFP), software and licenses
- Update and transfer ~~of~~ documentation currently in process
- Transfer ~~of~~ all ICE-specific software code in process
- Coordinate the transition process with DHS/ICE IT personnel
- Fully support the transition of ICE-specific requirements to any successor contractor
- Execute the TMP transition activities with no disruption in operational services.

4. Background

ICE is the largest investigative agency within DHS. Formed in 2003 as part of the Federal Government's response to the September 11, 2001 (9/11) attacks, ICE's primary mission is to protect national security, public safety and the integrity of the U.S. borders through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. ICE employs approximately 19,000 employees in over 400 offices worldwide with an annual budget of more than $5 billion. The agency's law enforcement authorities encompass more than 400 U.S. Federal statutes that ICE enforces in its commitment to ensuring national security and public safety.

HSI, a critical asset in the ICE mission, is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States. HSI investigations cover a broad range of areas with a particular emphasis on border related crime. This includes national security threats, financial and smuggling violations, counter-proliferation, weapons trafficking, financial crimes, import fraud, human trafficking, human smuggling,

narcotics trafficking, gang enforcement, child exploitation/pornography, child sex tourism, document fraud, critical infrastructure protection and immigration benefit fraud. HSI is responsible for modernizing the case management, subject record management and the interface functionality components of the legacy TECS system. This project will allow HSI to continue to successfully conduct criminal and administrative investigations toward its law enforcement mission.

TECS was developed in 1987 by the U.S. Customs Service as an umbrella system to support the business activities related to border crossing and investigative case management. Modernization of the functionality related generally to border crossing activities is currently being modernized by Customs and Border Protection (CBP), and is outside the scope of this effort. The ICE TECS Modernization program focuses, in general, on the investigative case management activities and ancillary functionality necessary to support the business requirements of HSI. The present system, also known as legacy TECS, is currently administered by the CBP Office of Information Technology (OIT). While the border crossing components (under modernization by CBP) and the investigative case management components (being modernized by ICE) are distinct modernization efforts, collaboration and interoperability of both the solutions and modernization efforts are essential to ensure mission success.

Legacy TECS (TECS was the acronym for the legacy Treasury Enforcement Communication System) is currently the backbone for recording, searching, managing, and maintaining law enforcement actions taken by CBP and ICE. Current TECS functionality does not allow interoperability among databases, modern interfaces for system users, or current security best practices.

4.1 Program Organization

The ICE TECS Modernization program is conducted under the direct oversight of ICE OCIO and the Executive Sponsor, HSI. The program is organized into an ICE TECS Modernization Program Office and a series of Integrated Project Teams (IPTs). Each IPT focuses on a critical portion of the program. An IPT comprises a team leader who is accountable for the team mission, objectives and deadlines, and IPT members who are key stakeholders with responsibility for a portion of the IPT objectives.

IPTs will be created, maintained and/or decommissioned based on program progression. Continuous coordination and communication between the various teams are essential and critical to the success of the program. The IPT structure provides defined roles and responsibilities to ensure accountability, enhance communication within the project, and enable more effective tracking of program goals and objectives by management. The IPTs work together to ensure that risks and issues are identified, addressed, and elevated when necessary. The Offeror shall provide information (e.g. status reports) and attend weekly reoccurring IPT meetings as required. Additionally the Offeror shall conduct trade studies and analysis in support of the IPTs as requested by the Government. The IPTs are currently organized as follows:

- **Requirements**. Responsible for managing requirements including refinement, categorization, and creation of new requirements where necessary.
- **Interfaces**. Responsible for implementing internal and external interfaces, establishing and maintaining communication with interface partners, and ensuring interface requirements are documented properly.
- **Data Migration Team**. Responsible for migrating legacy TECS data into a “target” database available for consumption by the ICM system provider. The Data Migration Team, in conjunction with HSI, will identify all legacy records required for ingestion into the ICM system.
- **Integration**. Responsible for coordinating integration among all the components of the ICE TECS Modernization system including data migration, HSI requirements, internal and external interfaces, and the ICM system. This team will serve as the release manager to ensure infrastructure availability and will coordinate deployments to environments throughout the system lifecycle.

- **Test**. Oversees implementation of the Test and Evaluation Master Plan (TEMP), which is provided as Exhibit G, and is responsible for overall integrated test planning and coordination.
- **Training and Communication**. Responsible for developing and delivering the training strategy, assisting in communications related to change management and leadership mobilization, developing a training and education plan, and communicating with the user community. The Offeror shall also provide some aspects of training for the ICM system (see Section 7.4).

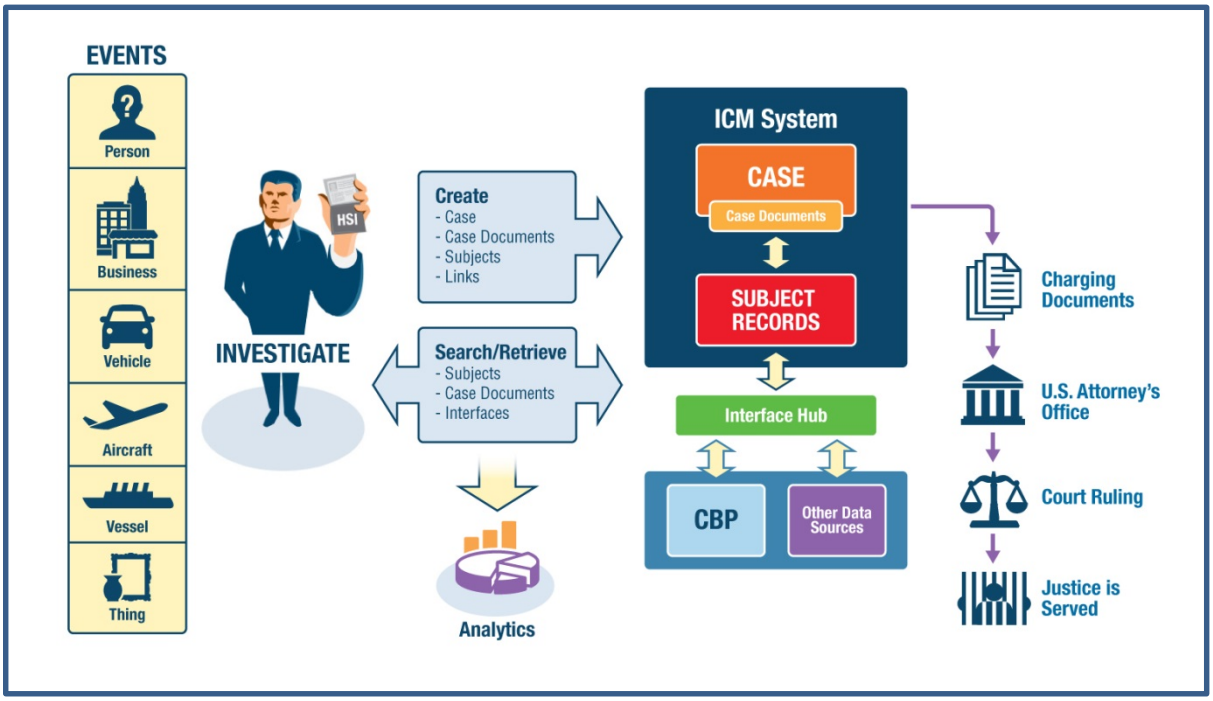
4.2 HSI Investigative Case Management Ecosystem View

The HSI Investigative Case Management Ecosystem View diagram shown in Figure 1 illustrates a reactive case initiated by an event and concluded upon reaching judicial process. This diagram shows the following ICM processes:

- Initiating an investigation beginning with an event or allegation
- Evaluating the event or allegation as it relates to potential criminal or administrative violations
- Documenting the initiation of the investigation by generating a case
- Conducting investigative activity involving searching and retrieving information internal to the ICM system that includes all types of subject records and other indices internal to ICE as well as external or interfaced systems and information, including CBP and other federal, state and local law enforcement partners
- Documenting investigative findings as part of the case
- Creating and documenting intelligence and other information related to the investigation
- Interfacing and utilizing analytical tools to further develop intelligence and investigative information
- Creating subjects records and passing lookouts* to CBP via the CBP lookout service
- Creating charging documents to facilitate prosecution in coordination with federal, state and local prosecutors.

*A lookout is an ICM system subject record shared with CBP for enforcement action and/or to support further investigations. Once shared, the lookout record becomes searchable and viewable by CBP according to defined access control permissions.

Figure 1: HSI Investigative Case Management Ecosystem View



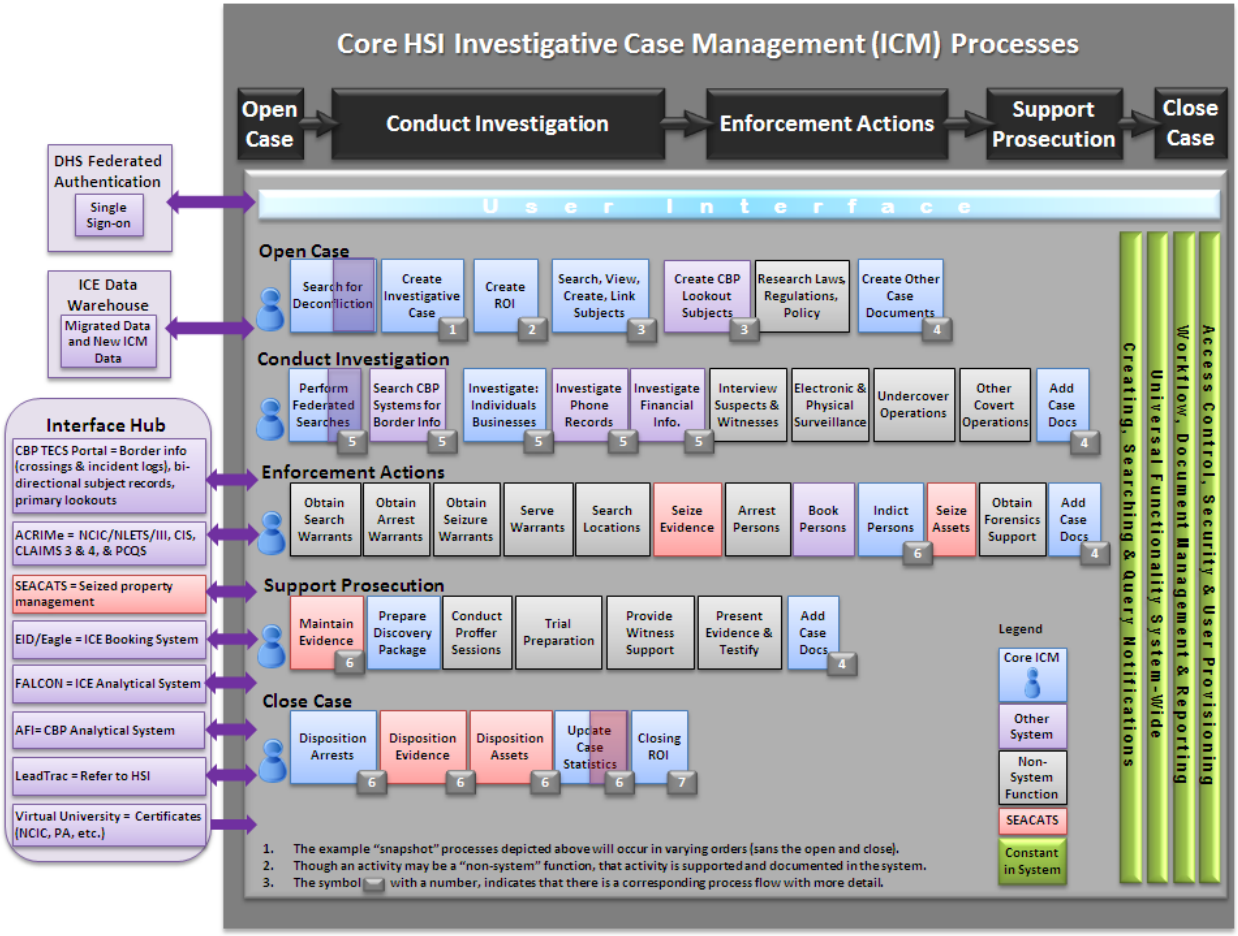
5. Mission Capabilities for the ICM System

The ICM system shall create, modify, close, query, view, print, and export ICE Investigative cases. The ICM system shall capture, store, and manage the data and other information relevant to ICE criminal and administrative investigations. The ICM system shall import legacy subject records and user data records from the ICE/CBP TECS mainframe system after the data has been migrated to an Oracle Relational Database Management System (RDBMS) by the ICE Data Migration Team.

Several high-level functional capability areas are described in this section to highlight some unique HSI requirements for the ICM system but are not intended to represent all HSI mission requirements. The Offeror shall meet the detailed requirements specified in Exhibit A.

Figure 2 is a high-level overview of HSI's core ICM processes and their relationship to other components of the ICE TECS Modernization system (e.g., the ICE Data Warehouse and the ICE interface hub). Also, Figure 2 shows the types of requirements that pertain to all ICM processes in the (green) vertical layers. More detailed HSI ICM processes, along with a mapping of HSI functional requirements to each process, are provided in Exhibit B.

Figure 2: CORE HSI Investigative Case Management Processes



5.1 Case Creation and Management

The ICM system shall create new ICE investigative cases. An investigative case is a "container" for numerous component documents/forms that support an investigation, such as the ROIs, internal management documents, subject records, and electronic surveillance data (ELSURs). The case is composed of metadata fields (such as program codes, case owner, supervisor name, etc.), a short narrative, and a hyperlinked link list of all records attached to the case and its numerous component documents.

The ICM system shall modify cases, close cases, and query/view/print/export cases. The ICM system shall capture, store, and manage data and other information relevant to ICE criminal and administrative investigations. The ICM system will not directly import legacy cases and component documents with the exception of subject records and user data records. However, the ICM system shall query legacy cases (which will be migrated to the ICE Data Warehouse). New cases created by the ICM system shall also be exported to the ICE Data Warehouse. The ICM system user shall be able to submit a single query that will return both legacy data and ICM system data and component documents in a consolidated result set.

5.2 Subject Record Management

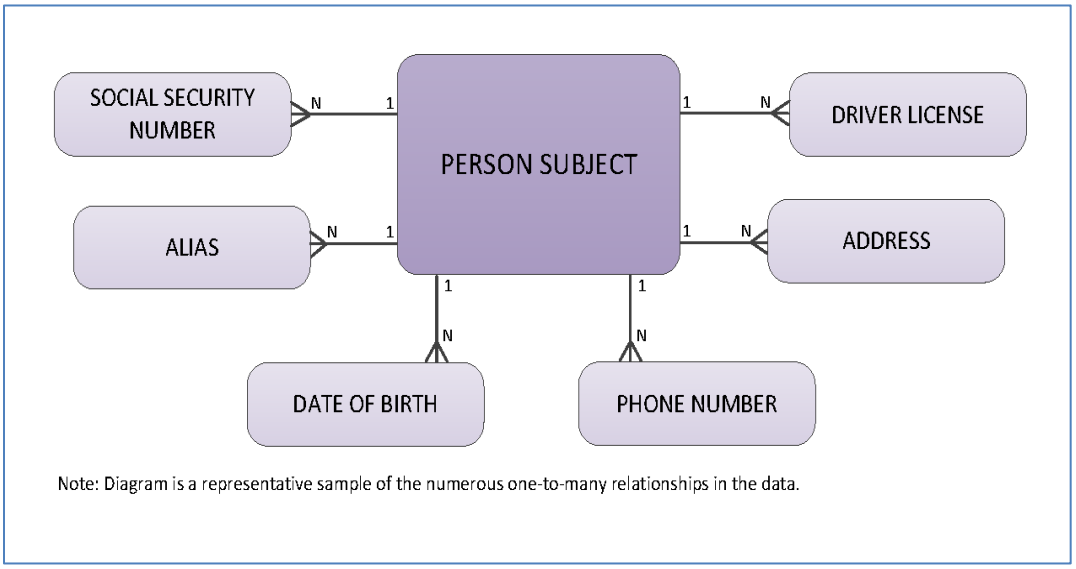
The ICM system shall create new subject records, modify subject records, query/view subject records, delete subject records, and print/export subject records. Subject record types shall include but should not

be limited to: Person, Business, Vessel, Vehicle, Aircraft, and Thing (a catchall type for other subject types).

The ICM system shall manage subject records allowing for: (1) an "entity" concept that enables multiple users to contribute to a communal set of identifying data about a subject (e.g., numerous users can add dates of birth for a single individual documented within the system); and (2) and the ability for each user to control his/her own data with individual access control rights. ICM system solutions that merely allow for a communal single record with shared rights will not meet this need, nor will solutions that facilitate the creation of multiple, duplicative records describing the same subject.

Due to the nature of their business, HSI agents collect most of the data elements on a subject of investigation in a one-to-many fashion. There are few attributes about a subject that are captured as a single instance value. The multiple values can be based on observations at various points in time, tips, falsified documents, etc. Each of the multiple values is considered a valid attribute, not deactivated or overwritten by more recently or more reliably obtained data. The ICM system shall make each value editable and searchable, both individually as well as in any combination of the one-to-many attributes that define the subject. For example, if a query on birthdate and social security number is run against all person subjects of investigation, a subject who has two birthdates and three social security numbers will be returned in the result set if there is a match with either one of the two birthdates and any one of his three social security numbers. Figure 3 provides a high-level view of one-to-many relationships in HSI subject records.

Figure 3: Example of One-to-Many Relationships in HSI Subject Records



5.3 Data Migration of Existing Legacy TECS Subject Records

Under a separate effort, the ICE TECS Modernization program will migrate HSI's legacy data from the TECS mainframe to an Oracle RDBMS (target database). The migrated data will contain all domains such as cases, ROIs, other case reports, subject records, and user data. The Oracle RDBMS will preserve the data cardinality and relationships among records.

The legacy cases and ROIs are considered "point-in-time" data and will not be required to be imported by the ICM system. However, subject records are the cornerstone of HSI's investigative process and shall be imported by the ICM system. Subject record-related access control and document links (subject-to-subject, subject-to-ROI, subject-to-case) will be available in the Oracle RDBMS, and shall also be imported and preserved in the ICM system with the subject record data.

User data and legacy access control data shall also be imported into the ICM system to associate record ownership and continue to support access control. The user data provides attributes about a user's organization and role within HSI and will tie in with ICE's single sign-on (SSO) mechanism.

Note that while other data domains (such as cases and ROIs) do not need to be imported by the ICM system, this information will be transferred to the ICE Data Warehouse during initial data migration. The ICM system shall search both the previous "point-in-time" data in the ICE Data Warehouse as well as newly created and managed ICM system data (i.e., new cases and ROIs) in a federated manner without requiring users to perform separate queries.

5.4 Reports of Investigation

The ROI has a unique workflow when compared to other case documents. The ICE agent who originated the ROI must also be the final author. That is, if a supervisor makes changes to the narrative of a submitted ROI, it is no longer considered a final draft for approval and would be routed back with the tracked changes/comments to the originating author in draft status.

Once an ROI is approved, the ICM system shall convert it to an Adobe PDF document and save it as the only version of the ROI. Earlier drafts of the ROI shall be eliminated. Once approved, no modifications to the narrative can be made by the operational user. However, a defined small subset of administrative users should have the ability to update or delete approved reports under limited circumstances.

The ROI differs from other documents in the system in that an ROI maintains both an "ROI author" and the "ROI owner." The ROI author can never change, even if the author is no longer a user provisioned in the ICM system. The ROI owner can change as follows: the "ROI owner" is always the current case agent for the case which contains the ROI. For example, if a user writes an ROI for his/her own case, but the case is later transferred to a different user, the ROI author will not change, but the ROI owner will become the new case agent. Likewise, if a user writes an ROI to another user's case, the ROI author and the ROI owner will be two different users.

The ICM system shall generate final, approved versions of all ROIs in the same template format (i.e., a standardized form with the same header, footer, and letterhead).

5.5 Notifications

The ICM system shall generate query and workflow-related notifications and send the notifications to ICE/HSI users to support ICE/HSI business processes. Query notifications shall be role based and adaptable to allow for notifications to occur or not occur based on defined circumstances. For example, the ICM system shall issue a query notification through email to a record owner of any queries conducted on his/her record, even if the record was not displayed because the querying user did not have access to the record.

The ICM system shall allow certain ICE user groups, for example ICE's internal affairs unit known as the Office of Professional Responsibility (OPR), to have special profiles that allow them to query records without generating query notifications to the record owner. ICM system users shall be able to set rules defining what does and does not trigger a query notification. Query and workflow notifications shall be provided by email. The query notification shall include information about the person conducting the query (both internal and external to ICE) and the path on which the record was viewed. If a record is queried by another HSI user, the notification shall indicate the date, time and location of the query. Additionally, the notification shall indicate the type of query and data the officer used to query the record. For example, a record owner would receive a notification that "HSI Special Agent John Smith queried your record on Jack Johnson from the San Antonio Texas field office by querying <last name>, <first name> and <date of birth>".

5.6 Interfaces

To support HSI operations, the ICM system shall interoperate with specified internal ICE and DHS systems and with specified systems external to DHS via data services provided by an ICE interface hub. In addition, the ICM system shall interface directly with the ICE Data Warehouse. The ICM system shall process transactions and updates that originate from external systems and shall share information with external systems through data services or open APIs. Additional information on interfaces is provided in the technical requirements section of this SOO.

5.7 Flexible Linking of Cases, Documents, and Subject Records

The ICM system shall link cases, documents and subject records to each other "vertically," "horizontally," and in a "nested" fashion. Individual document-level (or field-level) access control shall apply to linked records. The following examples describe each link category.

- **Vertically Linked:** Subject records, for example, are "contained" within a larger case by virtue of the fact that they have a many-to-one relationship with the case.
- **Horizontally Linked:** Records of the same document type can be linked to one another. For example, there can be "subject to subject" linking, where a Person subject record (PSR) is linked to a Business subject record because the person works at the business. Users shall be able to link these two subject record types in such a way that retrieving one of the records will cause the other linked records to be displayed (many-to-many relationship) in a "link list" for both records.
- **Nested:** An investigator may document an individual as a subject of his/her investigation in a PSR. The same investigator may also document a vehicle in a vehicle subject record (VSR) that will contain a series of fields to identify the owner of the vehicle. If during the course of investigation s/he learns that the vehicle is in fact owned by the person, the user will be able to "nest" the PSR "within" the VSR in such a way that the user would not need to perform dual entry by typing the owner's information in both the VSR's "car owner" fields as well as the creation of the VSR. The ICM system shall link the records together (many-to-many relationship) such that (1) the user does not need to perform dual entry and (2) the "nested" record will appear as such within the view of another record. From a technical perspective this is the same as horizontal linking with the addition of an intuitive user interface component and the re-population of data from one record type to another.

5.8 User Control of Access to Case-Related Information

The ICM system shall enable ICE/HSI users to control access of case-related information according to core user roles including: Case Agent, Case Supervisor, ROI Narrative Author, ROI Narrative Author's Supervisor, and other Supervisors. When a user searches for, or wishes to modify, records in the system, access to the records shall be based on the role of the user and the access control level set by the record owner(s).

The ICM system shall enable users to delegate responsibilities to other users. As an example, agents shall be able to open cases on behalf of other agents, and supervisors shall be able to delegate approval authority to other agents or supervisors when they are out of the office. Users shall be able to transfer documents to each other with supervisor approval. Also, multiple agents shall be able to contribute to a single work process; for example, several agents can write ROIs against a single user's case.

One unique HSI workflow requirement is the interaction between user roles and workflow states. For example, if an agent submits a report to his/her supervisor, the record shall be visible only to that agent and to the supervisor while in draft status. However, once the document is approved it shall become available to the larger HSI user community (within the confines of access control rules, which are specified by the document owner).

Exhibit F is a set of Responsible, Accountable, Consulted, Informed (RACI) charts that define ICE/HSI user roles in terms of who is responsible, accountable, consulted, and informed with regard to ICM system actions that may be taken by those users. The Offeror shall implement the detailed user role requirements described in these charts and in the requirements specified in Exhibit A.

5.9 Transfers of Users, Cases, and Subject Records

The ICM system shall handle transfers of HSI users, cases, and subject records according to the following business rules.

User Transfers: The ICM system shall not allow the reassignment of a user to a different office if that user's documents have not first been transferred to a different owner. The receiving owner must be assigned to the office associated with the documents to be transferred. For example, before agent Doe is transferred out of the New York office, his documents must first be transferred to another New York agent.

Case Transfers: The ICM system shall transfer (1) individual documents, including cases, subjects, ROIs and other case documents, to another user and (2) select several documents at once for transfer. If a case is transferred, the ICM system shall automatically transfer all linked documents. Note: An ROI always retains its original author.

Subject Record Transfers: The ICM system shall transfer unlinked subject records as a separate process from case transfer. The ICM system shall transfer subject records individually or several at once.

The ICM system shall check to make sure the receiving user is authorized to view all documents transferred to him/her. If the recipient does not have authorization for any document, the ICM system shall disallow the transfer and prompt the initiator to manually add the recipient to the list of authorized viewers for the document. This ensures that documents are not inadvertently transferred to unauthorized users.

Document transfers must be approved by the user's supervisor. As with all workflows in the system, the supervisor can both initiate a workflow and also approve the same workflow. (Thus, a supervisor can approve his/her own work.)

5.10 Searching Structured and Unstructured Data Across Document Types

The ICM system shall search both structured and unstructured data across multiple document types and possibly multiple systems internal and external to ICE and DHS. Structured data searches ensure consistency of search results within a specific search type, while unstructured or keyword searches provide the capability to search across structured data and narrative data (unstructured documents and free text contained within the narrative portion of a document). The ICM system shall include subject record search forms.

The following is an example of this essential capability with regard to structured data: addresses (and their constituent groups of fields) exist in multiple documents throughout the system, such as the person subject record, financial data (interface), CBP crossing data (interface), and other HSI and CBP subject record types. The user shall be able to conduct a consolidated address search that will match on all addresses regardless of the record type (internal or external to ICE/HSI) that contains them.

An ICM system user shall be able to search on the string "John Doe." This search shall return results where "John Doe" exists as a name on a form (structured) and/or the words "John Doe" appear in a narrative (unstructured). Users shall have the separate capability to search for "John Doe" as only a structured name within a specific record type.

5.11 Agent Work Hours

The ICM system shall enable HSI users to accurately document their hours worked each month, to include regular work hours, unscheduled overtime, undercover work hours, etc. The ICM system users shall be able to attribute the hours they enter to cases. The ICM system shall enable the user-entered hours to be accumulated and reported. For example, the ICM system shall report on the number of investigative hours spent on all narcotics cases involving methamphetamine. Also, the ICM system shall report granular elements such as hours worked by agent, by program code, etc.

6. Technical Capabilities for the ICM System

The Offeror shall meet the detailed requirements specified in Exhibit A. The following high-level technical capability areas highlight some important ICE/HSI requirements for the ICM system but are not intended to represent all technical requirements. The detailed requirements specified in Exhibit A take precedence if any deviations occur between requirements associated with the capability areas described in this section and the detailed requirements in Exhibit A.

6.1 Hosting Environments

Through a DHS private cloud environment, the ICE TECS Modernization program will have access to a pool of servers providing Virtual Machines (VMs) that can be used for the systems development life-cycle processes. The DHS cloud provides Development and Test as a Service (DTaaS) and Infrastructure as a Service (IaaS). The hosted environments include systems management, monitoring, security auditing, and 24/7 operations support as is provided for all other servers within the DHS enterprise data center. Available operating systems are RedHat Enterprise Linux 5 and 6, Windows Server 2008 R2, and Windows 7.

The Government will provide the infrastructure to all of the development teams supporting the ICE TECS Modernization program. Developer VMs can be ordered in several sizes suitable for uses that range from web servers to large database server/hosts, each with a choice of operating systems. The Government has identified requirements for at least nine (9) types of system environments to support the ICE TECS Modernization program as shown in Table 1.

Table 1. ICE TECS Modernization Program Hosting Environments

Environment	Purpose
Development (DEV)	Development environment (separate environments for major components of the ICE TECS Modernization system)
Development Integration (INT)	Integration and test environment
System Test (TST)	Formal system testing to validate integration and interoperability among all components
Performance Test (PERF)	Performance testing (load, capacity, response time)
User Acceptance Test (UAT)	User acceptance testing prior to deployment at IOC
Training (TRN)	User training and related documentation (ongoing)
Staging (STG)	Validation of deployment configuration prior to transition to production
Production (PROD)	Production environment
Disaster Recovery (DR)	Disaster recovery environment

The Offeror has the option to propose alternatives to the VM environments above to meet their hardware, software and overall performance requirements. However, given the compressed schedule, the Offeror should provide details on any proposed alternative implementation approach along with an associated risk mitigation plan and a detailed cost estimate (See RFP, Attachment 6-CLIN Structure, CLIN XX07).

6.2 Key Performance Parameters and Maintainability

Key performance parameters (KPPs) are specified for the ICE TECS Modernization system in the ICE TECS Modernization System Operational Requirements Document (ORD), which is provided as Exhibit E to the RFP. These KPPs are shown in Table 2. As the overall ICE TECS Modernization system includes several components, the Offeror shall meet the performance requirements relevant to their solution and its key role in the overall ICE TECS Modernization system.

In addition to the KPPs in Table 2, there are other performance requirements (e.g., related to maintainability) in the detailed requirements in Exhibit A. The availability KPP in Table 2 shall drive the ICM system maintainability requirements in terms of mean time to restore service (average time to restore service after a failure), mean downtime (time that the ICM system is not operational due to service incident or preventive maintenance including logistic and administrative delays), and planned downtime (time that the ICM system is not operational due to corrective and preventive maintenance including logistic and administrative delay time).

Table 2. KPPs for the ICE TECS Modernization System

No.	KPP	Threshold	Objective	Comments
1	**Response Time**: Transaction response time refers to the time required for completion of an individual transaction. Specifically, the time it takes from a workstation request to a workstation response, which is tested at the end user device level. Test time begins when the user hits enter after filling out the appropriate transaction criteria and ends when the intent of the transaction is accomplished, for example when search results appear on the results page. Response time for search includes responses from all data sources queried.	The system shall provide operationally acceptable transaction response time* for individual transactions across the system, not to exceed 5 seconds 95% of the time.	The system shall provide a transaction response time* for individual transactions across the system, not to exceed 3 seconds 99% of the time.	*Response time excludes transaction processing time on systems external to the investigative case management application. (For example, processing within the ICM application must not add more than 5 seconds to the time required for an external database to process a request with regard to Threshold or 3 seconds with regard to Objective.) Response time is calculated only for devices directly connected to an

No.	KPP	Threshold	Objective	Comments
				ICE network and does not include remote devices (i.e., connected through VPN, mobile device running over wireless network, etc.).
2	**Concurrent Users**: The system shall be able to handle a high level of users, measured by the number of concurrent users accessing the system at the same time.	No less than 6,000 users accessing the system at the same time with system capability allowing all users to conduct business transactions concurrently within the application.	No less than 10,000 users accessing the system at the same time with system capability allowing all users to conduct business transactions concurrently within the application.	Approximately 90% of system transactions are database reads. Database updates consists of the remaining 10%.
3	**Availability**: The ICM system shall achieve the required level of Operational Availability (Ao).	Ao > 99.07%	Ao > 99.97%	Required level of monthly Operational Availability for the ICM system components.

6.3 Measures of Effectiveness

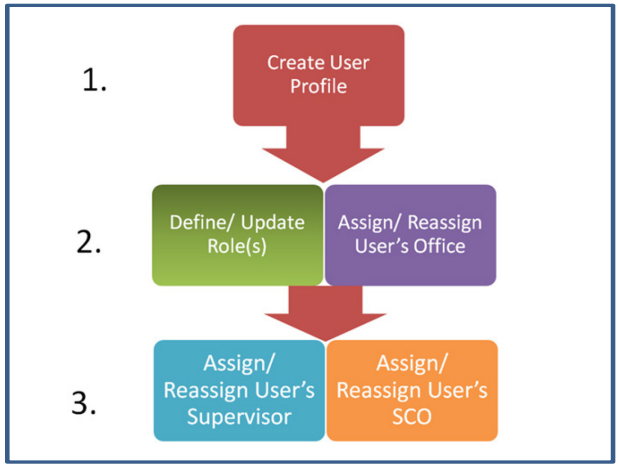
The following measures of effectiveness (MOEs) describe high-level capabilities pertaining to ICM system capability objectives the Offeror's proposed solution shall meet:

- Ability for all users with appropriate access to view cases and all associated documents, subject records, and links within five seconds of being created when they are accessing the system from a device directly connected to an ICE network
- Ability for users to create a lookout record and have that record available for posting to CBP TECS Portal within five seconds (via an ICE-developed data service)
- Ability for users to perform all work flow related to cases, case documents, and subject records (i.e., opening/creating, approving, modifying, deleting)
- Ability for users to link cases to case documents and subject records/lookouts
- Ability for users to link subject records/lookouts to case documents
- Ability of the ICM system to receive and present search responses from all sources with which the system interfaces within five seconds of the source data being made available to the ICM system
- Ability of the ICM system to generate audit trails to facilitate reconstruction of events on demand
- Reduced data entry time via elimination of duplicative requests for input of data from users
- Ability of the ICM system to interface with internal ICE/DHS systems and external systems as described in other sections of this SOO.

6.4 User Provisioning

New agents will need to be provisioned to the ICE Active Directory (AD) prior to being provisioned in the ICM system. This process is outside the scope of the ICM system user provisioning process. Once users are added to ICE AD, the process to provision a user to the ICM system can be initiated by an HSI System Control Officer (SCO) according to the three-step process shown in Figure 4. The process for updating user profiles follows these same steps. The steps are explained in more detail below.

Figure 4. HSI User Provisioning for the ICM System



Step 1: The SCO will create a user profile in the ICM system as follows:

- The SCO will enter user-name, middle-name, last name in a screen in the ICM system application
- The ICM system application will query ICE AD to retrieve user(s) matching this query
- The SCO will browse the list (if more than one is returned) and manually make a determination of which one of the users is most likely the individual he/she is intending to provision in the ICM system
- The SCO will then select that user from the list
- This completes the user-create process (some information from AD will be pre-populated in the screen).

Step 2: The SCO will then: a) define role(s) for this agent and b) assign an office code to this agent (this office code is based on an existing legacy office hierarchy).

Step 3: The SCO will then a) assign a supervisor to this user (filtered list of users based on the office selected) and b) assign a SCO user to this agent.

The ICM system shall develop a static office hierarchy of its own and host it in the ICM system database; therefore, a user's office information will not be retrieved from the ICE AD. Users will need to self-register upon initial logon to the ICM system. The ICM system shall present these users with a screen to update their personal information including their ICE email addresses.

The SSO process will use the ICE AD for initial user authentication. The ICM system shall then validate the user to the ICM system if that user has been provisioned in the ICM system user. Though all the ICM system users have an active ICE AD, not all ICE AD users have access to the ICM system. Merely having an active ICE AD, does not in and of itself mean a user can perform functions in the ICM system.

6.5 Single Sign On

The ICM system shall implement standards-based mechanisms, such as Security Assertion Markup Language (SAML 2.0), to achieve SSO within the DHS and ICE infrastructure. Authentication will be externalized to the ICM system. Oracle Access Manager is currently used as a proxy to AppAuth for Active Directory authentication of individual users. The ICM system shall implement industry standard Web Access Management (WAM) methods to enable SSO for application components of the ICM system.

6.6 Interfaces

The ICM system shall query and search specified data sources that are internal to ICE or DHS and external to DHS. Information shall be requested from interface partners by calling Simple Object Access Protocol (SOAP)-based web services exposed via the ICE Interface Hub which will be implemented by the ICE Interfaces Team. In addition, the ICM system shall interface directly with the ICE Data Warehouse. The ICM system shall authenticate and authorize individual users accessing interface services, and shall include the user's authenticated identity in each call for auditing purposes. The ICM system shall authenticate to the ICE Interface Hub using digital certificates and shall use secure socket layer (SSL) encrypted channels when transmitting or retrieving sensitive information via an interface. The ICM system shall process inbound interface information such as training and certification updates and asynchronous request notifications. Table 3 summarizes the interface operations that shall be supported by the ICM system.

Table 3. ICE TECS Modernization System Interfaces

Interface Title	Operation Description	Direction	End Point
AsyncResultNotification	NCIC/NLETS Result Notifications	Inbound (from the ICE Interface Hub)	ICM system
VUTrainingUpdate	User Profile Updates (Training Certifications)	Inbound (Update) (from the ICE Interface Hub, data will need to be persisted in ICM)	ICM system
SearchPersonSubject	ICM system provides various person attributes as query parameters and/or ranges as well as valid query targets. ICM may also provide a correlation ID for a response received from AsyncResultNotification.	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response, correlation ID in the event of asynchronous response, summary hit list, or exception message)

Interface Title	Operation Description	Direction	End Point
SearchVehicleSubject	ICM system provides various vehicle attributes as query parameters and/or ranges as well as valid query targets. ICM may also provide a correlation ID for a response received from AsyncResultNotification.	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response, correlation ID in the event of async response, summary hit list, or exception message)
SearchAircraftSubject	ICM system provides various aircraft attributes as query parameters and/or ranges as well as valid query targets. ICM may also provide a correlation ID for a response received from AsyncResultNotification.	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response, correlation ID in the event of async response, summary hit list, or exception message)
SearchVesselSubject	ICM system provides various vessel attributes as query parameters and/or ranges as well as valid query targets. ICM may also provide a correlation ID for a response received from AsyncResultNotification.	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response, correlation ID in the event of async response, summary hit list, or exception message)
SearchBusinessSubject	ICM system provides various business attributes as query parameters and/or ranges as well as valid query targets. ICM may also provide a correlation ID for a response received from AsyncResultNotification.	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response, correlation ID in the event of async response, summary hit list, or exception message)
SearchThingSubject	ICM system provides various thing attributes as query parameters and/or ranges as well as valid query targets. ICM may also provide a correlation ID for a response received from AsyncResultNotification.	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response, correlation ID in the event of async response, summary hit list, or exception message)

Interface Title	Operation Description	Direction	End Point
SearchSubscriber	ICM system provides various telephone subscriber attributes as well as query targets (Falcon/TLS is expected to be only valid target for IOC)	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response, summary hit list, or exception message).
SearchPenRegister	ICM system provides telephone digit information as well as query targets (Falcon/TLS is expected to be only valid target for IOC)	Outbound (Query/Search)	ICE Interface Hub (responds with detail query response [including related case numbers], summary hit list, or exception message).
GetCaseStatistics	ICM system provides case and 151/incident information as parameters	Outbound (Query/Search)	ICE Interface Hub (responds with updated incident information, preliminary case statistics, and final case statistics retrieved from CBP SEACATS or associated CBP data stores)
SearchEvent	ICM system provides event centric query parameters, such as flight parameters, border crossing, arrest, seizures, financial transactions, financial declarations (CMIR), shipments (cargo).	Outbound (Query/Search)	ICE Interface Hub (responds with matching event information as linked subject information as available from the queried target. Subsequent queries may be required to retrieve detailed subject information)
CreateSubjectLookout	ICM system provides all required subject attribute information (for all supported subject types), lookout status, as well as query and lookout notification conditions.	Outbound (Update)	ICE Interface Hub (responds with CBP TECS Subject ID, Date/Time Subject Lookout update confirmed [if placed on lookout])

Interface Title	Operation Description	Direction	End Point
UpdateSubjectLookout	ICM system provides CBP TECS Subject Identifier and Lookout Status Updates (ON/OFF Lookout, Lookout Level) and lookout notification conditions. This operation is used to place existing subjects on lookout as well as remove them from lookout.	Outbound (Update)	ICE Interface Hub (responds with CBP TECS Subject ID, Date/Time Subject Lookout update confirmed [if placed on lookout])
ReceiveEventNotification	Allows ICM to be made aware of *subscribed* law enforcement events and information related to cases and/or investigative subjects, such as seizures, arrests, border crossings, and other information.	Inbound (from the ICE Interface Hub)	ICM system

6.7 Data Migration

Table 4 provides a high-level description of the ICE/HSI user data and subject domains that will be migrated from the legacy TECS system to a target database and, from there, imported into the ICM system. In addition to the database tables shown in Table 4, there are 11 global reference tables that are shared across domains and there are other reference tables that support ICM system functionality (e.g., cases and documents) even though the associated legacy TECS data is not being migrated into the ICM system. All these reference tables shall be migrated from the legacy TECS system and imported into the ICM system. The data model for the target database is provided as Exhibit C to this RFP.

Table 4. Legacy TECS Data to be Migrated to the ICM System

Data Domain/ Document	Description	No. of Tables	No. of Assoc. Ref Tables	Record Count in Base Table
User Profile	User attributes that define access control, document creation, workflow, notifications, etc.	7 tables: 1 base plus 6 child	38 tables	35K
Access Control	Read, write, and approval restrictions that are defined on each document.	3 tables: 1 base plus 2 child	7 tables	4.7M

Data Domain/ Document	Description	No. of Tables	No. of Assoc. Ref Tables	Record Count in Base Table
Person Subject	Tables for a Person Subject record (dependent on supertype).	28 tables: 1 base plus 27 child	26 tables	3.4M
Vehicle Subject	Tables for a Vehicle Subject record (dependent on supertype).	8 tables: 1 base plus 7 child	3 tables	565K
Business Subject	Tables for a Business Subject record (dependent on supertype).	16 tables: 1 base plus 15 child	4 tables	607K
Aircraft Subject	Tables for an Aircraft Subject record (dependent on supertype).	10 tables: 1 base plus 9 child	8 tables	24K
Vessel Subject	Tables for a Vessel Subject record (dependent on supertype).	12 tables: 1 base plus 11 child	1 table	51K
Thing Subject	Tables for a Thing Subject record (dependent on supertype).	13 tables: 1 base plus 12 child	4 tables	14K
Subject-Case Links	Table for associating a Subject with a Case.	1 table		4.8M
Subject-ROI Links	Table for associating a Subject with an ROI.	1 table		6.7M
Subject-Subject Links	Table for associating a Subject with another Subject.	1 table		7.6M

Two general kinds of permission are used in the legacy TECS system: (1) read access to records and (2) access to transactions that may alter the records.

Each subject record in the legacy TECS system may be assigned one of three access levels:

Level 1. All users have access

Level 3. Users belonging to one or more specified groups have access

Level 4. Access is limited to specified users.

Access level 2, which limits access to a certain agency, is available but not used for subject records.

Transactions can be assigned to a user via a profile code or through direct association. Typically, a user will be assigned a profile code that gives the user membership in a set of groups or permission to execute a set of transactions. The direct assignment of a group or transaction is unusual, can be performed only by privileged users, and is likely to be temporary.

6.8 ICE Data Warehouse

The ICM system shall use SQL or a web service to extract data for all HSI domains from the ICE Data Warehouse. The ICM system shall receive multiple queries per day to meet near real-time reporting requirements. In order to minimize impact to transactional processing in the ICM system, the ICM system shall identify database changes since the last extraction of data to refresh the ICE Data Warehouse. For example, the ICM system might use separate views, tables, or flat files holding only the information added or updated since the last refresh time. New or updated records shall be labeled by the ICM system via created/updated time stamps on all records.

The ICM system shall access the ICE Data Warehouse to conduct searches for legacy data not imported into the ICM system. The ICE Data Warehouse will retrieve legacy data (e.g., cases and ROIs) as well as new data created by the ICM system, and return results back in an XML file. The ICE Data Warehouse will have mechanisms to enforce access control and will only return results to which requesting users have access. The ICM system shall render the results from the ICE Data Warehouse in MS-Word, PDF, or similar formats.

6.9 Security and Privacy

The system shall be compliant with all relevant security controls outlined in the Federal Information Processing Standard (FIPS) and the Federal Information Security Management Act (FISMA) to include, but not limited to, the ability of the federal government to perform a security certification and accreditation process to obtain an authorization to operate that will be signed by the federal principal without delay to system deployment. Specific security and privacy requirements for the ICM system are specified in the detailed ICM system requirements provided as Exhibit A to the RFP.

DHS/ICE has determined that all Offerors/subcontractor(s) performing work under the ICE TECS Modernization contract will have access to sensitive but unclassified (SBU) DHS and ICE information, which requires DHS Suitability Clearance 5C (Moderate Risk) position of public trust adjudication.

6.10 Licensing and Data

Any software proposed by the Offeror for use to develop ICE's ICM system shall be approved by the Government before any purchase or use. The Licensee of any such software product shall be ICE. License agreements shall be provided to ICE for final review to ensure the terms of the license agreement are consistent with federal law and will meet ICE's needs. The Offeror shall ensure that it has complied with Section H requirements pertaining to licensing before it will be approved for use in development of ICM.

Any data input by ICE, or its support contractors, into the ICM system shall remain ICE property and ICE retains ownership of said data. If the ICM system is based upon a COTS solution, then ICE anticipates that the system will be modified to address ICE's ICM system requirements. Any software modifications made to the system under this contract shall be provided to the government with unlimited rights. Unlimited rights means that the Government has unlimited rights to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so as defined in FAR 27.401. ICE shall also obtain unlimited rights in any other data first produced in performance of this contract, form fit, and function data and all other data delivered under the contract other than restricted rights in commercial computer software. If the ICE system is based upon a Government Off the Shelf solution, ICE also anticipates that the system will need to be modified to address ICE's ICM system requirements. ICE

shall have unlimited rights to all software modifications as defined above and shall have the same rights in the GOTS solution as the Government previously acquired when the GOTS software was developed.

ICE shall retain ownership of any training plans and manuals, all data input in the system, and all outputs of the system including all investigative reports created by a User of the system. Outputs of the system include both the data and formatting of the outputs. The Offeror shall not attach any unauthorized or restricted markings on this material. This material shall be delivered IAW FAR 52.227-17.

7. Implementation and Management

The overall ICE TECS Modernization program will follow structured DHS-approved lifecycle implementation processes as outlined in the ICE System Lifecycle Management (SLM) Handbook and will refer to the ICE Technical Reference Model (TRM) for commercial products already approved by ICE. The ICE TRM is provided as Exhibit I to the RFP. The Offeror shall conduct an implementation strategy, in collaboration with the Government that aligns with the ICE SLM Handbook and industry best practices for managing programs and projects. During ICM system implementation and management, the Offeror shall collaborate closely with the Government and other developers on the ICE TECS Modernization program. In particular, the Offeror shall provide the Government with complete visibility and transparency into all phases of their implementation and management work on the ICE TECS Modernization program, including working co-located with the Government, conducting daily collaboration with Government counterparts, both technical and functional, sharing of status on a real-time basis via joint contractor/Government teams. Such collaboration will enable the Government to determine acceptance (or not) of the technology and functionality being development efficiently and effectively.

7.1 Development, Test, and Deployment Approach

DHS/ICE will provide the hosting environments described in Table 1 (Section 6.1) to support development, test, and deployment activities for all ICE TECS Modernization system components, including the ICM system unless otherwise proposed by the Offeror and approved by the Government.

The Offeror shall use these hosting environments for development, configuration, integration, and testing of their solution. (Note that Section 6.1 in this SOO allows the Offeror to propose alternatives to the DHS/ICE hosting environments.) The Offeror shall be responsible for all demonstration testing to verify that its' system is working properly prior to submitting it for integration. The Offeror shall participate in all levels of integration and testing as the overall ICE TECS Modernization system progresses to IOC. Specifically, the Offeror shall assist in analyzing problems discovered during all levels of integration and testing. The Offeror shall correct errors and shortfalls (example of shortfall is not meeting performance requirements) in the ICM system during all levels of integration and testing.

Software code changes applied to the Offeror's system to support the ICM system requirements shall be developed to be compatible with, and shall not prevent the ability to apply, future software maintenance upgrades to the Offeror's product that are made generally available. In general, the Government would prefer that functional extensions or enhancements and error corrections developed for the ICM system during all development, test, and maintenance activities be incorporated into the code base for the ICM system so that future releases will include these changes. Code developed by the Offeror for ICE shall require approval by the Government to be incorporated into the ICM system code base. The Government shall have unlimited rights to any code developed by the Offeror specifically for ICE and not incorporated into the ICM system code base.

7.2 Service Desk Support.

The Offeror shall support the ICE TECS Modernization system service desk as described below.

Tier 1. The Government will provide Service Desk Tier 1 support for the overall ICE TECS Modernization system. The Offeror shall be responsible for Tier 2 and 3 system support for the ICM system and for assisting with the overall problem resolution of the ICE TECS Modernization system.

Tier 2. All problems that cannot be resolved at the Tier 1 support level will be automatically turned over to Tier 2 System Maintenance and Support to be handled as follows:

- The status of the problem ticket shall be reported using an ICE approved tracking tool
- Typical Tier 2 activities include patching systems, running scripts, and applying minor fixes
- A feedback loop will be developed such that systemic issues identified during Tier 2 and Tier 3 escalation procedures will be routinely evaluated and reviewed with the appropriate project manager to assess the need for a System Change Request (SCR) for incorporation into a future release
- If Tier 2 System Maintenance Support cannot resolve the assigned ticket or perform the required tasks, then the ticket shall be referred to the Tier 3 System Maintenance and Support.

Tier 3. Software, performance, and implementation failures will be identified and evaluated and the level of effort associated with requests for system modification will be estimated. Corrective work includes generating SCRs that reflect the need to correct a component, re-integrate components to develop a revised version of the overall system or revised version of a major component in the system, and perform all levels of test on the revised version. Or, SCRs may indicate the need to change requirements or technical specifications. Problems addressed at the Tier 3 level will likely require updating the Systems Engineering Lifecycle (SELC) documentation as necessary. Tier 3 service desk support activities should be handled as follows:

- All maintenance activities that reach this level will have an SCR opened and be reported using the ICE approved tracking tool
- SCRs will be prioritized and approved in writing by authorized Government personnel and entered into the ICE approved management tracking tool
- Prior to commencing a system modification, ICE TECS Modernization system service desk contractors and the OCIO IT project manager will determine the degree of the modification as minor, moderate, or major and ICE approved processes for SCRs will be followed.

Tier 2 and Tier 3 Support standard hours of operation will be Monday through Friday 8:00 am and 8:00 pm Eastern Standard Time (EST), excluding Government holidays as designated by the United States Office of Personnel Management (OPM). Table 5 summarizes Tier 2 and 3 performance requirements.

Table 5. Tier 2 and 3 Performance Requirements

Tasks	Metric	Service Level	How it will be Measured
Tier 2 and Tier 3 Software Support	Response time for Tier 2 and Tier 3 tickets during standard support hours	No more than 1 hour	Time the ticket is assigned to Tier 2 or Tier 3 until the time the ticket is picked up for action.
Tier 2 and Tier 3 Software Support	Resolution time of Tier 2 and Tier 3 tickets	5 business calendar days	Time the ticket is placed in the Tier 2 or Tier 3 queue for action to the time it appears as closed or deferred as a future candidate for release.
Tier 2 and Tier 3 Software Support	Response time for emergency tickets after hours	No more than 1 hour	Time the ticket is assigned as an emergency until the time the ticket is picked up for action.

7.3 Maintenance Support

The Offeror shall provide their approach for maintenance of the ICM system solution for maintenance periods that will be executed in 12-month (or remainder thereof) options for the remaining period of performance (i.e., the balance of 48 months remaining after IOC).

This approach would include the Offeror's basic approach to ICM system bug fixes/patches, routine maintenance and upkeep of the ICM system solution, licenses and upgrades on the Offeror supplied products associated with the ICM solution, and upgrade frequency for the installed ICM system solution.

7.4 Training Strategy

The Offeror shall describe all existing training plans and materials, user guides, operations manuals, and maintenance manuals for their ICM system solution and shall provide these training-related items to the Government. The Offeror shall provide subject matter expertise regarding the proposed solution, its function, and corresponding training/user readiness lessons learned to support the Government in developing the training program for the ICM system.

7.5 Systems Engineering Lifecycle Documentation

The ICE TECS Modernization Program will follow a COTS integration implementation pattern for the ICE SELC Tailoring Plan provided as Exhibit D to the RFP. The Offeror shall produce the Work Products and Deliverables described in Exhibit H to the RFP.

The Offeror shall deliver draft versions, revised versions, and final versions of required system documents. The Offeror shall provide deliverables electronically, virus free and in the acceptable electronic format mutually agreed to by the Government and Offeror.

7.6 Project Management

The Offeror shall collaborate with the Government and other contractors on all aspects of the ICE TECS Modernization program to help achieve all objectives and requirements outlined or identified in this SOO

and other components of the RFP. The Offeror shall manage the ICM system implementation project using industry best practices including:

- **Status Reporting**. Weekly reports of status related to development, testing, staffing, issues, and risks including date of completion during the IOC timeframe.
- **Communication**. Due to the interrelationship of the various development, testing, training and deployment activities, the Offeror's project management activities shall include plans to build relationships among all organizations involved in the ICE TECS Modernization program.
- **Risk Management**. All systems development projects have inherent risks. Given the visibility of this project, the Offeror will be incorporated into the Program's risk management process, logging all risks and mitigation strategies into a centralized Risk Register and meeting weekly to discuss them to determine if they should become elevated risks. The ICE TECS Modernization program will maintain oversight of all program risks via a risk review board chaired by the Government program manager.
- **Configuration Management**. The Offeror shall be responsible for the configuration management activities associated with all aspects of implementing the ICM system, from initial installation through final Government acceptance and during all levels of system integration and test.
- **Quality Assurance**. The Offeror shall provide a Quality Assurance Surveillance Plan (QASP) that outlines how the quality of the work associated with implementing the ICM system will be assured.
- **IPT Support.** The Offeror shall provide information (e.g. status reports) and attend weekly reoccurring IPT meetings as described in Section 4.1.

7.7 Key Personnel

The Government requests a commitment letter for the following personnel to support the Offeror's performance on the ICE TECS Modernization program during the IOC timeframe. All key personnel shall be intimately familiar with the specific ICM product proposed by the Offeror and shall have been involved in key leadership roles during previous installations, configurations, and extensions to meet customer requirements.

Project Manager

The Offeror's Project Manager shall have relevant experience in managing the implementation of large complex programs that involve working with other contractors to produce the overall system required by the Government. The Project Manager shall work with the Government Program Manager, the Government Contracting Officer, and other Government and contractor personnel to ensure that the technical solutions and schedules are implemented according to the agreed upon schedule. The Project Manager shall ensure the Offeror's staff works with the Government and other contractors on the ICE TECS Modernization program to perform horizontal integration planning and all phases of implementation, test, and deployment.

Principal Systems Architect

The Offeror's Principal Systems Architect shall have relevant experience in analyzing all requirements pertaining to complex computer systems and developing architectures to guide the design of the system. Such architectures should include software, hardware, databases, communications, and security and privacy mechanisms to satisfy the total set of functional and technical requirements and to be scalable and extensible to accommodate future requirements for the system. The Principal Systems Architect shall be knowledgeable about, and experienced in developing, open system architectures, applying industry architecture-related standards, and using reference models to further describe the architecture.

Principal Systems Engineer

The Offeror's Principal Systems Engineer shall have relevant experience in all aspects of planning, analysis, design, and development of complex computer systems. The Principal Systems Engineer shall be knowledgeable about, and experienced in, the analysis of business/mission, technical, performance, security and privacy requirements; system and component implementation methodologies and tools; data modeling and data processing; integration; cross-system interoperability; and all aspects of testing large complex systems that comprise components from multiple vendors and developers.

Principal Software Development Manager

The Offeror's Principal Software Development Manager shall have relevant experience in all aspects of system and software requirements analysis, system and software design to meet functional and non-functional requirements (including performance, scalability, extensibility, security, privacy), software development, interface development, component integration and testing, subsystem integration and testing, cross-system integration and testing, data modeling and database design, and software quality assurance. The Principal Software Development Manager should be familiar with detailed aspects of setting up and managing hosting environments for all phases of development and testing, and production.

8. Applicable Documentation

The Offeror shall comply with the Exhibits to this RFP (which provide more details on requirements and implementation processes) and the latest versions of all technology standards and architecture policies, processes, and procedures applicable to the overall ICE TECS Modernization program. These publications include, but are not limited to, the following:

Exhibits Referenced in the SOO

- Exhibit A: ICE/HSI Investigative Case Management System Requirements (Law Enforcement Sensitive)
- Exhibit B: ICE/HSI Business Process Deep Dive Diagrams (Law Enforcement Sensitive)
- Exhibit C: Target Data Model for Data Migration (Law Enforcement Sensitive)
- Exhibit D: ICE TECS Modernization SELC Tailoring Plan
- Exhibit E: ICE TECS Modernization ORD
- Exhibit F: ICE/HSI RACI Charts (Law Enforcement Sensitive)
- Exhibit G: ICE TECS Modernization TEMP
- Exhibit H: ICM System Table of Work Products and Deliverables
- Exhibit I: ICE TRM

Other References Relevant to the SOO

- DHS 4300A Sensitive Systems Policy Directive, Version 8.0, Dated March 14, 2011 http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf
- DHS MD 4010.2 (DRAFT), Section 508 Program Management Office & Electronic and Information Technology Accessibility, Issued 10/26/2005, http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_40102_section_508_program_management_office_and_information_technology_accessibility.pdf

- Final FAR Rule for Implementing Section 508 of the Rehab Act Electronic and Information Technology Accessibility for Persons with Disabilities, Document Date: 07/11/2013, http://www.section508.gov/documents/final-far-rule-implementing-section-508-rehab-act
- ICE Architecture Test and Evaluation Plan – Available upon request
- ICE Enterprise Systems Assurance Plan – Available upon request
- ICE System Lifecycle Management (SLM) Handbook – Available upon request
- ICE Technical Reference Model (It is understood that the proposed TECS Modernization ICM system would be reviewed as an emerging technology within the ICE SLM and TRM/Information Technology Change Request processes) – Available upon request
- NIST FIPS 201-2 ―Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
- *NIST SP 800-63-1: Electronic Authentication Guideline* (December 2011), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910006
- OMB M-06-16 ―Acquisition of Products and Services for Implementation of HSPD-12, June 23, 2006, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf
- OMB M-10-15 ―FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, Issued April 21, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors" , February 3, 2011, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
- Privacy Act of 1974, http://www.justice.gov/opcl/privstat.htm
- Federal Information Processing Standard (FIPS) 199 http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Federal Information Security Management Act (FISMA), November 22, 2002 http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Appendix A - List of Acronyms

Acronym	Description
AD	Active Directory
CBP	Customs and Border Protection
CLIN	Contract Line Item Number
COTS	Commercial Off-the-Shelf
CWBS	Contractor Work Breakdown Structure
DHS	Department of Homeland Security
DTaaS	Development Test as a Service
FOC	Full Operational Capability
GFE	Government Furnished Equipment
GFP	Government Furnished Property
HSI	Homeland Security Investigations
IaaS	Infrastructure as a Service
ICE	Immigration and Customs Enforcement
ICM	Investigative Case Management
IOC	Initial Operational Capability
IPT	Integrated Project Team
KPP	Key Performance Parameter
MOE	Measure of Effectiveness
NCIC	National Crime Information Center
NLETS	National Law Enforcement Telecommunications Systems
O&M	Operations and Maintenance
OCIO	Office of Chief Information Officer
OIT	Office of Information Technology
OPR	Office of Professional Responsibility
POP	Period of Performance
PSR	Person Subject Record
PWS	Performance Work Statement
RACI	Responsible, Accountable, Consulted, Informed
RDBMS	Relational Database Management System
RFP	Request for Proposal
ROI	Reports of Investigation

Acronym	Description
SAML	Security Assertion Markup Language
SCI	Sensitive Compartmented Information
SCO	System Control Officer
SELC	Systems Engineering Life Cycle
SLM	System Lifecycle Management
SOO	Statement of Objectives
SSO	Single Sign On
TECS	Treasury Enforcement Communication System
TEMP	Test and Evaluation Master Plan
TLS	Telephone Linking System
TMP	Transition Management Plan
TRM	Technical Reference Model
VM	Virtual Machine
VPN	Virtual Private Network
VSR	Vehicle Subject Record
WAM	Web Access Management