INFORMATION SHARING ENVIRONMENT (ISE)

FUNCTIONAL STANDARD (FS)

SUSPICIOUS ACTIVITY REPORTING (SAR)

VERSION 1.0

1. Authority. The National Security Act of 1947, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); DNI memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law.

2. Purpose. This issuance serves as the initial functional standard for ISE-SARs, and constitutes the first of the *Common Terrorism Information Sharing Standards (CTISS)* issued by the PM-ISE.

3. Applicability. This ISE-FS applies to all departments or agencies that possess or use terrorism or homeland security information, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, consistent with Section 1016(i) of the IRTPA.

4. References. *ISE Implementation Plan*, November 2006; *ISE Enterprise Architecture Framework (EAF)*, August 2007; *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment*, Version 1.0; *ISE-AM-300: Common Terrorism Information Standards Program*, 31 October 2007; *Common Terrorism Information Sharing Standards Program Manual*, Version 1.0, October 2007; National Information Exchange Model, *Concept of Operations*, Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23.

5. Definitions.

a. *Artifact:* Detailed mission product documentation addressing information exchanges and data elements for SAR (data models, schemas, structures, etc.).

b. *Common Terrorism Information Sharing Standards (CTISS):* Business process-driven, performance-based "common standards" for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. Two categories of common standards are formally identified under CTISS: functional standards and technical standards. Functional standards set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.

Technical standards document specific technical methodologies and practices to design and implement information sharing capability into ISE systems. CTISS, such as ISE-SAR, are implemented in ISE participant infrastructures that include ISE Shared Spaces as described in the ISE EAF.

c. *Information Exchange:* The transfer of information from one organization to another organization, in accordance with CTISS processes.

d. *ISE-Suspicious Activity Report (ISE-SAR):* An ISE-SAR is a SAR (as defined below in 5g) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

e. *National Information Exchange Model (NIEM):* A joint technical and functional standards program initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) that supports national-level interoperable information sharing.

f. *Privacy Field:* A data element that may be used to identify an individual and, therefore, may be subject to privacy protection.

g. *Suspicious Activity Report:* Official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.

h. *Universal Core (UCore):* A joint technical standard that defines a small set of context-free data elements for loosely-coupled information sharing at the national level.

6. Guidance. This functional standard is hereby established as the initial functional standard for ISE-SARs. It is based on documented information exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs by ISE participants.

7. Responsibilities.

a. The PM-ISE, in consultation with the Information Sharing Council (ISC), will:

(1) Maintain and administer this ISE-SAR Functional Standard, to include:

(a) Updating the business process and information flows for ISE-SAR.

(b) Updating data elements and product definitions for ISE-SAR.

(2) Publish and maintain configuration management of this ISE-SAR Functional Standard.

(3) Assist with the development of ISE-SAR implementation guidance and governance structure, as appropriate, to address privacy, policy, architecture, and legal issues.

(4) Work with ISE participants, through the CTISS Committee, to develop a new or modified ISE-SAR Functional Standard, as needed.

(5) Coordinate, publish, and monitor implementation and use of this functional standard, and coordinate with the White House Office of Science and Technology Policy and with the National Institute of Standards and Technology (in the Department of Commerce) for broader publication, as appropriate.

b. Each ISC member and other affected department or agency shall:

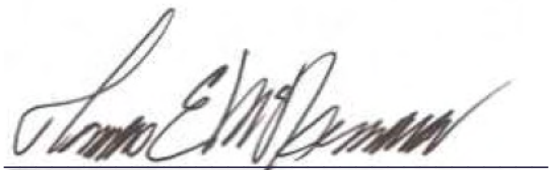
(1) Propose updates to the PM-ISE for this functional standard, as appropriate.

(2) As appropriate, incorporate this ISE-SAR Functional Standard, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g. operations and maintenance {O&M} or enhancements).

(3) As appropriate, incorporate this ISE-SAR Functional Standard, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission specific programs, systems, or initiatives (e.g. development, modernization, or enhancement {DME}).

(4) Ensure incorporation of this ISE-SAR Functional Standard, as set forth in 7b(2) or 7b(3) above, is done in compliance with ISE Privacy Guidelines and any additional guidance provided by the ISE Privacy Guidelines Committee.

8. Effective Date and Expiration. This ISE-FS is effective immediately and will remain in effect as the initial functional standard for ISE-SAR until updated, superseded, or cancelled.



Program Manager for the
Information Sharing Environment

Date: January 25, 2008

This page intentionally blank.

PART A – ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I – DOCUMENT OVERVIEW

A. List of ISE-SAR Information Exchange Artifacts

The full ISE-SAR information exchange contains four types of supporting artifacts. This documentation provides details of implementation processes and other relevant reference materials. A synopsis of the functional standard artifacts is contained in Table 1 below.

Table 1 – Functional Standard Artifacts[1]

Artifact Type	Artifact	Artifact Description
Development and Implementation Tools	1. Component Mapping Template (CMT) (SAR-to-NIEM/UCore)	This spreadsheet captures the ISE-SAR information exchange class and data element (source) definitions and relates each data element to corresponding National Information Exchange Model (NIEM) Extensible Mark-Up Language (XML) elements and UCore elements, as appropriate.
	2. NIEM Wantlist	The Wantlist is an XML file that lists the elements selected from the NIEM data model for inclusion in the Schema Subset. The Schema Subset is a compliant version to both programs that has been reduced to only those elements actually used in the ISE-SAR document schema.
	3. XML Schemas	The XML schema provides a technical representation of the business data requirements. They are a machine readable definition of the structure of an ISE-SAR-based XML Message.
	4. XML Sample Instance	The XML Sample Instance is a sample document that has been formatted to comply with the structures defined in the XML Schema. It provides the developer with an example of how the ISE-SAR schema is intended to be used.

[1] Development and implementation tools may be accessible through .www.ise.gov . Additionally, updated versions of this functional standard will incorporate the CTISS Universal Core which harmonizes the NIEM Universal Core with the DoD/IC UCore.

SECTION II – SUSPICIOUS ACTIVITY REPORTING EXCHANGES

A. ISE-SAR Purpose

This ISE-SAR Functional Standard is designed to support the sharing of suspicious activity, incident, or behavior (hereafter referred to as activity) information that has a potential terrorism nexus throughout the Information Sharing Environment (ISE) and between State and major urban area fusion centers and their law enforcement,[2] homeland security,[3] or other information sharing partners at the Federal, State, local, and tribal levels to the full extent permitted by law. ISE-SARs will provide for the discovery of patterns, trends, or nationally suspicious activities beyond what would be recognized within a single jurisdiction, state, or territory. Standardized and consistent sharing of suspicious activity information with the State and major urban area fusion centers is deemed vital to assessing, deterring, preventing, or prosecuting those planning terrorist activities. This ISE-SAR Functional Standard has been designed to incorporate key elements for terrorist related activities and may be potentially leveraged by other communities for other crimes.

B. ISE-SAR Scope

Suspicious activity is defined as "*observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention*." An ISE-SAR requires a two-part process to determine that a SAR has a potential terrorism nexus. Some examples of the criteria for identifying SAR as having a potential terrorism nexus are listed below, but a more comprehensive list can be found in Part B (ISE-SAR Criteria Guidance).

- Surveillance
- Photography of facilities
- Site breach or physical intrusion
- Cyber attacks
- Probing of security

It is also important to acknowledge that many terrorist activities are now being funded via local or regional crimes organizations. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious activities, behavior, or materials as a byproduct or secondary element to a criminal enforcement or investigation activity. This means that, while some ISE-SARs may document activities or incidents to which local agencies have already responded, they are being shared to facilitate aggregate trending or analysis.

---

2 All references to Federal, State, local and tribal law enforcement are intended to encompass civilian law enforcement, military police, and other security professionals.

3 All references to homeland security are intended to encompass public safety, emergency management, and other officials who routinely participate in the State or major urban area's homeland security preparedness activities.

The Suspicious Activity Reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities. The ISE-SAR effort offers a standardized means for feeding information repositories and data analysis tools. Any patterns identified during ISE-SAR data analysis may be investigated in cooperation with the reporting agency or the State or major urban area fusion center.

C. ISE-SAR Top-level Business Processes & Activities

Beginning with the observation and documentation of a suspicious activity, there are five necessary top-level processes—some of which are primarily organizational specific and others with broader implications for the ISE—that together comprise the ISE Suspicious Activity Reporting Process. These processes have been categorized as listed below and are graphically depicted in Figure 1.

1. Information acquisition
2. Organizational processing
3. Integration/consolidation
4. Data retrieval/distribution
5. Feedback

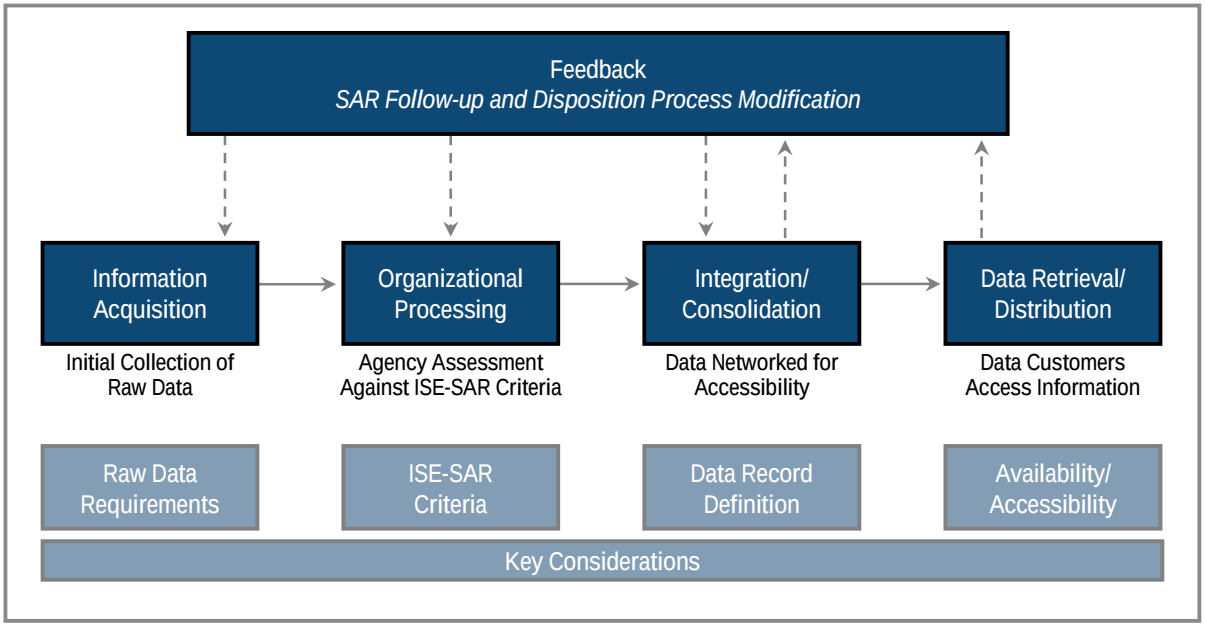


Figure 1 – ISE-SAR Top-level Process

1. Information Acquisition

Information Acquisition includes the activities that transpire between observation of a suspicious activity and the point at which the suspicious activity has been entered into an organizational or agency ISE-SAR reporting process.

There are numerous approaches to collecting and documenting these observations which vary by discipline and agency. For instance, one local law enforcement organization may initially capture all suspicious activity observations via its standard Field Interview Card or Report which, upon identification or validation as a SAR, would later be flagged for ISE-SAR processing. Another local law enforcement officer may instead directly input suspicious activity observation into a SAR interface, tips and leads, or other reporting system where it could be identified and validated as an ISE-SAR.

For the ISE-SAR *Information Acquisition* business phase, the focus for the ISE should not be to standardize all aspects of the various organization-specific analytical processes or systems, but to instead focus on ensuring specific information deemed necessary by ISE-SAR consumers can be acquired, reflected through an organization's process whenever possible, and shared appropriately. This information is codified into data elements which are atomic units of data with associated attributes. These attributes include a data element name which uniquely identifies this piece of information such as "Person First Name" and a definition to describe the type of information that should be stored using this data element.

2. Organizational Processing

The *Organization Processing* category of processes involves assessing whether an event should be deemed a suspicious activity.

Each contributing organization has its own processes to review and validate SAR information. For example, in some cases, information is reviewed by a supervisor and/or other subject matter expert before being advanced; while in other organizations, a quality assurance review is also required. The majority of the processes in the *Organizational Processing* category are specific to each ISE participant constructed to support participant missions to include, but not limited, to terrorism. While modification of some of the processes may be necessary to conform to overall ISE functional standards, the primary focus of the ISE in this business process category is to establish common criteria to ensure potential terrorism-related SAR information is placed into the ISE.

3. Integration/Consolidation

The *Integration/Consolidation* category of processes involves making the individual agency or department's SAR information available for integration in the ISE through ISE Shared Spaces as described in the ISE EAF. The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria. Second, based on available knowledge and information, the analyst or law enforcement

officer determines whether the information meeting the criteria may have a nexus to terrorism. Once SAR information has been identified as potentially terrorism-related, an ISE participant would share that information, specifically the "data elements," with the State or major urban area fusion center and the broader ISE community.

4. Data Retrieval/Distribution

This process category involves those activities that will allow departments, agencies, and ISE participants to receive or retrieve ISE-SARs from across the ISE population.

5. Feedback

This final ISE-SAR process category captures three types of feedback designed to improve the overall quality and effectiveness of the ISE-SAR process.

1. **Utilization:** This entails the requirement for a mechanism to inform the originating organization if SAR information is utilized or requires modifications to clarify, update, or correct information.

2. **Cross-flow/Back-flow:** This entails a mechanism to link SARs, and to reflect this information in the ISE to give end-users the ability to follow-up on the report.

3. **Process Modification:** This entails adding to, clarifying, or modifying the SAR data elements being collected; the criteria being utilized to nominate SARs to the ISE; and other ISE-SAR process issues.

D. Broader ISE-SAR Applicability

Consistent with ISE Privacy Guidelines and Presidential Guideline 2, and to the full extent permitted by law, this ISE-SAR Functional Standard is designed to support the sharing of unclassified information or controlled unclassified information (CUI) within the ISE.[4] There is also a provision for using a data element indicator for designating classified national security information as necessary. The State or major urban area fusion centers shall act as the key conduit between the State, local, and tribal (SLT) agencies and other ISE participants. It is also important to note the ISE Shared Space[5] implementation concept is focused exclusively on terrorism related information, however many SAR originators and consumers have responsibilities beyond terrorist activities and beyond the scope of the ISE. Of special note, there is no intention to modify through this ISE-SAR Functional Standard or otherwise affect the currently supported and/or mandated direct interactions between State, local, and tribal law enforcement and investigatory personnel and the Joint Terrorism Task Force (JTTF) or Field Intelligence Groups (FIGs).

---

4 The Presidential Guideline 3 Report: Standardize Procedures for Sensitive But Unclassified (SBU) information is currently in the final interagency review process. For purposes of this ISE-SAR Functional Standard, the term Controlled Unclassified Information is intended to cover unclassified information that carries a control marking.

5 Program Manager-ISE, *ISE Enterprise Architecture Framework, Version 1.0*, (Washington, DC: PM-ISE, 2007), xviii.

This ISE-SAR Functional Standard should be used as the ISE-SAR information exchange standard for all ISE participants. Although the extensibility of this functional standard does support customization for unique communities, jurisdictions wishing to modify this functional standard must carefully consider the consequences of customization. The PM-ISE requests that modification follow a formal change request process through the SAR governance process (to be adopted) and CTISS Committee under the Information Sharing Council, for both community coordination and consideration. Furthermore, messages that do not conform to this functional standard may not be consumable by the receiving organization and may require modifications by the nonconforming organizations.

There exist a variety of internal processes conducted at the State and major urban area fusion centers and their external interfaces to the Federal Government. Figure 2 represents a number of the various information management and exchange processes that take place in the reporting and sharing of suspicious activities. As shown, SAR vetting and standards is one part of a number of processes that support the functional flow of information in the ISE.

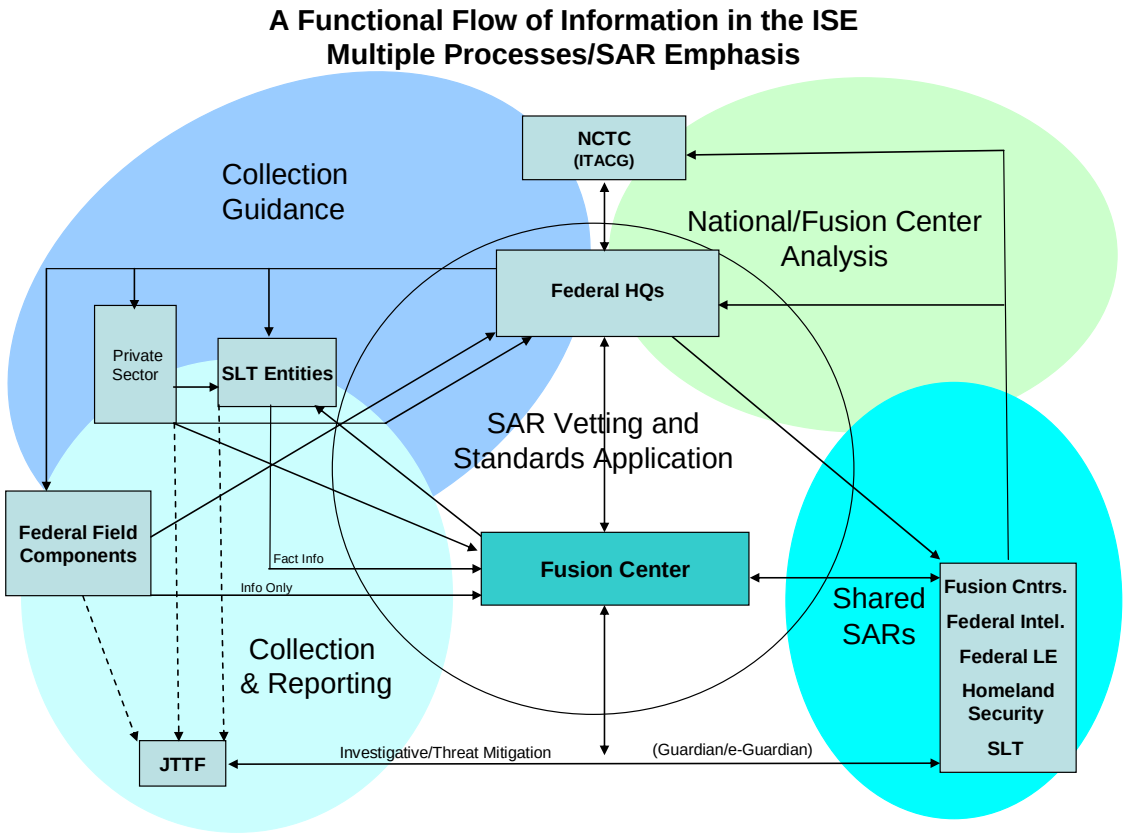


Figure 2 – ISE-SAR Exchanges

E. Protecting Privacy

Laws that prohibit or otherwise limit the sharing of personal information vary considerably between the Federal, State, and local levels. The Privacy Act of 1974 (5 USC §552a) as amended, other statutes such as the E-Government Act, and many government-wide or departmental regulations establish a framework and criteria for protecting information privacy in the Federal Government. The ISE must facilitate the sharing of information in a lawful manner, which by its nature must recognize, in addition to Federal statues and regulations, different state and local or tribal laws and statutes that affect privacy. One method for protecting privacy while enabling the broadest possible sharing, would be to anonymize ISE-SAR reports by removing data elements that contain personal information. Accordingly two ISE-SAR information exchange packages have been created; a "Detailed" and a "Summary" ISE-SAR package. ISE-SAR exchanges can employ either the "Detailed" or "Summary" SAR information exchange depending on the sending or receiving agencies' laws, regulations, and other data sharing requirements. The difference between these two exchanges lies in the inclusion or exclusion of certain data elements that may be used to identify an individual, i.e., "privacy fields."

The "Detailed" ISE-SAR information exchange includes all law enforcement defined data elements *including* privacy fields such as name, address, and vehicle registration information. The "Summary" ISE-SAR information exchange includes the aforementioned law enforcement defined data elements *excluding* privacy fields such as name, address, and vehicle registration information. Each ISE participant can exclude additional data elements from the summary ISE-SAR information exchange in accordance with its own legal and policy requirements. It is believed the data contained within a "Summary" ISE-SAR will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the sending agency. Because of variances of data expected within ISE-SAR exchanges, only the minimum elements are considered mandatory. These are enumerated in the READ ME document in the technical artifacts folder that is part of this ISE-SAR Functional Standard.

It is important to note that implementers can employ either information exchange and still populate only those data elements that are compatible with local statute and policy. As the ISE evolves, it may be possible to specifically identify those privacy fields common to all jurisdictions, enabling development of a standardized summary ISE-SAR. Currently, the privacy fields identified in the ISE-SAR exchange data model (Section IV, below) are the minimum fields that should be removed from a 'Detailed' ISE-SAR.

SECTION III – INFORMATION EXCHANGE DEVELOPMENT

This ISE-SAR Functional Standard is a collection of artifacts that support an implementer's creation of ISE-SAR information exchanges, whether "Detailed" or "Summary." The basic ISE-SAR information exchange is documented using four unique artifacts giving implementers tangible products which can be leveraged for local implementation. A domain model provides a graphical depiction of those data elements required for implementing an exchange and the cardinality between those data elements. Second, a Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element.

Third, information exchanges include the schemas which consist of a document, extension, and constraint schema. Fourth, at least one sample XML Instance and associated style-sheet is included to help practitioners validate the model, mapping, and schemas in a more intuitive way.

SECTION IV – ISE-SAR EXCHANGE DATA MODEL

A. Summary of Elements

This section contains a full inventory of all ISE-SAR information exchange data classes, elements, and definitions. Items and definitions contained in cells with a light purple background are data classes, while items and definition contained in cells with a white background are data elements. A wider representation of data class and element mappings to source (ISE-SAR information exchange) and target is contained in the Component Mapping Template located in the technical artifacts folder.

Cardinality between objects in the model is indicated on the line in the domain model (see Section 5A). Cardinality indicates how many times an entity can occur in the model. For example, Vehicle, Vessel, and Aircraft all have cardinality of 0..n. This means that they are optional, but may occur multiple times if multiple suspect vehicles are identified.

Clarification of Organizations used in the exchange:

- The **Source Organization** is the agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The Source Organization will not change throughout the life of the SAR.
- The **Submitting Organization** is the organization providing the ISE-SAR to the ISE. The Submitting Organization and the Source Organization may be the same.
- The **Owning Organization** is the organization that owns the target associated with the suspicious activity.

Table 2 – ISE-SAR Information Exchange Data Classes, Elements, and Definitions

Privacy Field	Source Class/Element	Source Definition
	Aircraft	
	Aircraft Engine Quantity	The number of engines on an observed aircraft.
	Aircraft Fuselage Color	A code identifying a color of a fuselage of an aircraft.
	Aircraft ID	A unique identifier assigned to the aircraft by the observing organization—used for referencing. [free text field]
	Aircraft Make Code	A code identifying a manufacturer of an aircraft.
	Aircraft Model Code	A code identifying a specific design or type of aircraft made by a manufacturer.
	Aircraft Style Code	A code identifying a style of an aircraft.
	Aircraft Tail Number	An identifier of an aircraft. Sometimes referred to as a tail number. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Aircraft Wing Color	A code identifying a color of the wings of an aircraft.
	Attachment	
	Attachment Type Text	Describes the type of attachment (e.g., surveillance video, mug shot, evidence). [free text field]
	Binary Image	Binary encoding of the attachment.
	Capture Date	The date that the attachment was created.
	Description Text	Text description of the attachment. [free text field]
	Format Type Text	Format of attachment (e.g., mpeg, jpg, avi). [free text field]
	Attachment URI	Uniform Resource Identifier (URI) for the attachment. Used to match the attachment link to the attachment itself. Standard representation type that can be used for Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).
	Attachment Privacy Field Indicator	Identifies whether the binary attachment contains information that may be used to identify an individual.
	Contact Information	
	Person First Name	Person to contact at the organization.
	Person Last Name	Person to contact at the organization.
	E-Mail Address	An email address of a person or organization. [free text field]
	Full Telephone Number	A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument. [free text field]
	Driver License	
	Expiration Date	The date the document expires.
	Issuing Authority Text	Code identifying the organization that issued the driver license assigned to the person. Examples include Department of Motor Vehicles, Department of Public Safety and Department of Highway Safety and Motor Vehicles. [free text field]
X	Driver License Number	A driver license identifier or driver license permit identifier of observed person of interest involved with the suspicious activity. [free text field]
	Follow-Up Action	
	Activity Date	Date that the follow-up activity started.
	Activity Time	Time that the follow up activity started.
	Assigned By Text	Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations. [free text field]
	Assigned To Text	Text describing the person or sub-organization that will be performing the designated action. [free text field]
	Disposition Text	Description of disposition of suspicious activity investigation. [free text field]
	Status Text	Description of the state of follow-up activity. [free text field]
	Location	
	Location Description	A description of a location where the suspicious activity occurred. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Location Address	
	Building Description	A complete reference that identifies a building. [free text field]
	County Name	A name of a county, parish, or vicinage. [free text field]
	Country Name	A country name or other identifier. [free text field]
	Cross Street Description	A description of an intersecting street. [free text field]
	Floor Identifier	A reference that identifies an actual level within a building. [free text field]
	Mile Marker Text	Identifies the sequentially numbered marker on a roadside that is closest to the intended location. Also known as milepost, or mile post. [free text field]
	Municipality Name	The name of the city or town. [free text field]
	Postal Code	The zip code or postal code. [free text field]
	State Name	Code identifying the state.
	Street Name	A name that identifies a particular street. [free text field]
	Street Number	A number that identifies a particular unit or location within a street. [free text field]
	Street Post Directional	A direction that appears after a street name. [free text field]
	Street Pre Directional	A direction that appears before a street name. [free text field]
	Street Type	A type of street, e.g., Street, Boulevard, Avenue, Highway. [free text field]
	Unit ID	A particular unit within the location. [free text field]
	Location Coordinates	
	Altitude	Height above or below sea-level of a location.
	Coordinate Datum	Coordinate system used for plotting location.
	Latitude Degree	A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive).
	Latitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Latitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Degree	A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).
	Longitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Observer	
	Observer Type Text	Indicates the relative expertise of an observer to the suspicious activity (e.g., professional observer versus layman). Example: a security guard at a utility plant recording the activity, or a citizen driving by viewing suspicious activity. [free text field]
X	Person Employer ID	Number assigned by an employer for a person such as badge number. [free text field]
	Owning Organization	

Privacy Field	Source Class/Element	Source Definition
	Organization Item	A name of an organization that owns the target. [free text field]
	Organization Description	A text description of organization that owns the target. The description may indicate the type of organization such as State Bureau of Investigation, Highway Patrol, etc. [free text field]
X	Organization ID	A federal tax identifier assigned to an organization. Sometimes referred to as a Federal Employer Identification Number (FEIN), or an Employer Identification Number (EIN). [free text field]
	Organization Local ID	An identifier assigned on a local level to an organization. [free text field]
	Other Identifier	
X	Person Identification Number (PID)	An identifying number assigned to the person, e.g., military serial numbers. [free text field]
	PID Effective Date	The date that the PID number became active or accurate.
	PID Expiration Date	The date that the PID number expires.
	PID Issuing Authority Text	The issuing authority of the identifier. This may be a state, military organization, etc.
	PID Type Code	Code identifying the type of identifier assigned to the person. [free text field]
	Passport	
X	Passport ID	Document Unique Identifier. [free text field]
	Expiration Date	The date the document expires.
	Issuing Country Code	Code identifying the issuing country. [free text field]
	Person	
X	AFIS FBI Number	A number issued by the FBI's Automated Fingerprint Identification System (AFIS) based on submitted fingerprints. [free text field]
	Age	A precise measurement of the age of a person.
	Age Unit Code	Code that identifies the unit of measure of an age of a person (e.g., years, months). [free text field]
	Date of Birth	A date a person was born.
	Ethnicity Code	Code that identifies the person's cultural lineage.
	Maximum Age	The maximum age measurement in an estimated range.
	Minimum Age	The minimum age measurement in an estimated range.
X	State Identifier	Number assigned by the state based on biometric identifiers or other matching algorithms. [free text field]
X	Tax Identifier Number	A 9-digit numeric identifier assigned to a living person by the U.S. Social Security Administration. A social security number of the person. [free text field]
	Person Name	
X	First Name	A first name or given name of the person. [free text field]
X	Last Name	A last name or family name of the person. [free text field]
X	Middle Name	A middle name of a person. [free text field]
X	Full Name	Used to designate the compound name of a person that includes all name parts. This field should only be used when the name cannot be broken down into its component parts or if the information is not available in its component parts. [free text field]

Privacy Field	Source Class/Element	Source Definition
X	Moniker	Alternative, or gang name for a person. [free text field]
	Name Suffix	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, or otherwise qualifies the name. [free text field]
	Name Type	Text identifying the type of name for the person. For example, maiden name, professional name, nick name.
	Physical Descriptors	
	Build Description	Text describing the physique or shape of a person. [free text field]
	Eye Color Code	Code identifying the color of the person's eyes.
	Eye Color Text	Text describing the color of a person's eyes. [free text field]
	Hair Color Code	Code identifying the color of the person's hair.
	Hair Color Text	Text describing the color of a person's hair. [free text field]
	Person Eyewear Text	A description of glasses or other eyewear a person wears. [free text field]
	Person Facial Hair Text	A kind of facial hair of a person. [free text field]
	Person Height	A measurement of the height of a person.
	Person Height Unit Code	Code that identifies the unit of measure of a height of a person. [free text field]
	Person Maximum Height	The maximum measure value on an estimated range of the height of the person.
	Person Minimum Height	The minimum measure value on an estimated range of the height of the person.
	Person Maximum Weight	The maximum measure value on an estimated range of the weight of the person.
	Person Minimum Weight	The minimum measure value on an estimated range of the weight of the person.
	Person Sex Code	A code identifying the gender or sex of a person (e.g., Male or Female).
	Person Weight	A measurement of the weight of a person.
	Person Weight Unit Code	Code that identifies the unit of measure of a weight of a person. [free text field]
	Race Code	Code that identifies the race of the person.
	Skin Tone Code	Code identifying the color or tone of a person's skin.
	Clothing Description Text	A description of an article of clothing. [free text field]
	Physical Feature	
	Feature Description	A text description of a physical feature of the person. [free text field]
	Feature Type Code	A special kind of physical feature or any distinguishing feature. Examples include scars, marks, tattoo's, or a missing ear. [free text field]
	Location Description	A description of a location. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Registration	

Privacy Field	Source Class/Element	Source Definition
	Registration Authority Code	Text describing the organization or entity authorizing the issuance of a registration for the vehicle involved with the suspicious activity. [free text field]
X	Registration Number	The number on a metal plate fixed to/assigned to a vehicle. The purpose of the license plate number is to uniquely identify each vehicle within a state. [free text field]
	Registration Type	Code that identifies the type of registration plate or license plate of a vehicle. [free text field]
	Registration Year	A 4-digit year as shown on the registration decal issued for the vehicle.
	ISE-SAR Submission	
	Additional Details Indicator	Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.
	Data Entry Date	Date the data was entered into the reporting system (e.g., the Records Management System).
	Dissemination Description Code	Generally established locally, this code describes the authorized recipients of the data. Examples include Law Enforcement Use, Do Not Disseminate, etc.
	Fusion Center Contact First Name	Identifies the first name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Last Name	Identifies the last name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact E-Mail Address	Identifies the email address of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Telephone Number	The full phone number of the person at the fusion center that is familiar with the record (e.g., law enforcement officer).
	Message Type Indicator	e.g., Add, Update, Purge.
	Privacy Purge Date	The date by which the privacy information will be purged from the record system; general observation data is retained.
	Privacy Purge Review Date	Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR record.
	Submitting ISE-SAR Record ID	Identifies the Fusion Center ISE-SAR Record identifier for reports that are possibly related to the current report. [free text field]
	ISE-SAR Title	Plain language title (e.g., Bomb threat at the “X” Hotel). [free text field]
	ISE-SAR Version	Indicates the specific version of the ISE-SAR that the XML Instance corresponds. [free text field]
	Source Agency Case ID	The case identifier for the agency that originated the SAR. Often, this will be a local law enforcement agency. [free text field]
	Source Agency Record Reference Name	The case identifier that is commonly used by the source agency—may be the same as the System ID. [free text field]
	Source Agency Record Status	The current status of the record within the source agency system.

Privacy Field	Source Class/Element	Source Definition
	Privacy Information Exists Indicator	Indicates whether privacy information is available from the source fusion center. This indicator may be used to guide people who only have access to the summary information exchange as to whether or not they can follow-up with the originating fusion center to obtain more information.
	Sensitive Information Details	
	Classification Label	A classification of information. Includes Confidential, Secret, Top Secret, no markings. [free text field]
	Classification Reason Text	A reason why the classification was made as such. [free text field]
	Sensitivity Level	Local information security categorization level (Controlled Unclassified Information-CUI, including Sensitive But Unclassified or Law Enforcement Sensitive). [free text field]
	Tearlined Indicator	Identifies whether a report is free of classified information.
	Source Organization	
	Organization Name	The name used to refer to the agency originating the SAR. [free text field]
	Organization ORI	Originating Agency Identification (ORI) used to refer to the agency.
	System ID	The system that the case identifier (e.g., Records Management System, Computer Aided Dispatch) relates to within or the organization that originated the Suspicious Activity Report. [free text field]
	Source Agency Contact First Name	The first name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Last Name	The last name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Email Address	The email address of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Phone Number	The full phone number of the person at the agency that is familiar with the record (e.g., law enforcement officer).
	Suspicious Activity Report	
	Community Description	Describes the intended audience of the document. [free text field]
	Community URI	The URL to resolve the ISE-SAR information exchange payload namespace.
	LEXS Version	Identifies the version of Department of Justice LEISP Exchange Specification (LEXS) used to publish this document. ISE-FS-200 has been built using LEXS version 3.1. The schema was developed by starting with the basic LEXS schema and extending that definition by adding those elements not included in LEXS. [free text field]
	Message Date/Time	A timestamp identifying when this message was received.
	Sequence Number	A number that uniquely identifies this message.
	Submitting Organization	
	Organization Name	Common Name of the fusion center or ISE participant that submitted the ISE-SAR record to the ISE. [free text field]
	Organization ID	Fusion center or ISE participant's alpha-numeric identifier. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Organization ORI	ORI for the submitting fusion center or ISE participant. [free text field]
	System ID	Identifies the system within the fusion center or ISE participant that is submitting the ISE-SAR. [free text field]
	Suspicious Activity	
	Activity End Date	The end or completion date in Greenwich Mean Time (GMT) of an incident that occurs over a duration of time.
	Activity End Time	The end or completion time in GMT of day of an incident that occurs over a duration of time.
	Activity Start Date	The date in GMT when the incident occurred or the start date if the incident occurs over a period of time.
	Activity Start Time	The time of day in GMT that the incident occurred or started.
	Observation Description Text	Description of the activity including rational for potential terrorism nexus. [free text field]
	Observation End Date	The end or completion date in GMT of the observation of an activity that occurs over a duration of time.
	Observation End Time	The end or completion time of day in GMT of the observation of an activity that occurred over a period of time.
	Observation Start Date	The date in GMT when the observation of an activity occurred or the start date if the observation of the activity occurred over a period of time.
	Observation Start Time	The time of day in GMT that the observation of an activity occurred or started.
	Tip Class Code	Broad category of threat to which the tip or lead pertains. Includes Financial Incident, Suspicious Activity, and Cyber Crime.
	Tip Subtype Text	Breakdown of the Tip Type, it indicates the type of threat to which the tip or lead pertains. The subtype is often dependent on the Tip Type. For example, the subtypes for a nuclear/radiological tip class might be Nuclear Explosive or a Radiological Dispersal Device. [free text field]
	Tip Type Code	Indicates the type of threat to which the tip or lead pertains. Examples include a biological or chemical threat.
	Weather Condition Details	The weather at the time of the suspicious activity. The weather may be described using codified lists or text.
	Target	
	Critical Infrastructure Indicator	Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
	Infrastructure Sector Code	The broad categorization of the infrastructure type. These include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

Privacy Field	Source Class/Element	Source Definition
	Infrastructure Tier Text	Provides additional detail that enhances the Target Sector Code. For example, if the target sector is Utilities, this field would indicate the type of utility that has been targeted such as power station or power transmission. [free text field]
	Structure Type Code	National Data Exchange (N-DEx) Code that identifies the type of Structure that was involved in the incident.
	Target Type Text	Describes the target type if an appropriate sector code is not available. [free text field]
	Structure Type Text	Text for use when the Structure Type Code does not afford necessary code. [free text field]
	Target Description Text	Text describing the target (e.g., Lincoln Bridge). [free text field]
	Vehicle	
	Color Code	Code that identifies the primary color of a vehicle involved in the suspicious activity.
	Description	Text description of the entity. [free text field]
	Make Name	Code that identifies the manufacturer of the vehicle.
	Model Name	Code that identifies the specific design or type of vehicle made by a manufacturer—sometimes referred to as the series model.
	Style Code	Code that identifies the style of a vehicle. [free text field]
	Vehicle Year	A 4-digit year that is assigned to a vehicle by the manufacturer.
X	Vehicle Identification Number	Used to uniquely identify motor vehicles. [free text field]
X	US DOT Number	An assigned number sequence required by Federal Motor Carrier Safety Administration (FMCSA) for all interstate carriers. The identification number (found on the power unit, and assigned by the U.S. Department of Transportation or by a State) is a key element in the FMCSA databases for both carrier safety and regulatory purposes. [free text field]
	Vehicle Description	A text description of a vehicle. Can capture unique identifying information about a vehicle such as damage, custom paint, etc. [free text field]
	Related ISE-SAR	
	Fusion Center ID	Identifies the fusion center that is the source of the ISE-SAR. [free text field]
	Fusion Center ISE-SAR Record ID	Identifies the fusion center ISE-SAR record identifier for reports that are possibly related to the current report.
	Relationship Description Text	Describes how this ISE-SAR is related to another ISE-SAR. [free text field]
	Vessel	
X	Vessel Coast Guard Document Number	An identifying number assigned by the U.S. Coast Guard to commercial vessels and certain motor yachts over five tons. Number is encompassed within valid marine documents and permanently marked on the main beam of a documented vessel. [free text field]
X	Vessel ID	A unique identifier assigned to the boat record by the agency—used for referencing. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Vessel ID Issuing Authority	Identifies the organization authorization over the issuance of a vessel identifier. Examples of this organization include the State Parks Department and the Fish and Wildlife department. [free text field]
	Vessel Make	Code that identifies the manufacturer of the boat.
	Vessel Model	Model name that identifies the specific design or type of boat made by a manufacturer—sometimes referred to as the series model.
	Vessel Model Year	A 4-digit year that is assigned to a boat by the manufacturer.
	Vessel Name	Complete boat name and any numerics. [free text field]
	Vessel Overall Length	The length measurement of the boat, bow to stern.
	Vessel Overall Length Measure	Code that identifies the measurement unit used to determine the boat length. [free text field]
X	Vessel Serial Number	The identification number of a boat involved in an incident. [free text field]
	Vessel Type Code	Code that identifies the type of boat.
	Vessel Propulsion Text	Text for use when the Boat Propulsion Code does not afford necessary code. [free text field]

B. Association Descriptions

This section defines specific data associations contained in the ISE-SAR data model structure. Reference Figure 3 (UML-based model) for the graphical depiction and detailed elements.

Table 3 – ISE-SAR Data Model Structure Associations

Link Between Associated Components	Target Element
Link From Suspicious Activity Report to Attachment	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityAttachmentLinkAssociation
Link From Suspicious Activity Report to Sensitive Information Details	Hierarchical Association
Link From Suspicious Activity Report to ISE-SAR Submission	Hierarchical Association
Link From Suspicious Activity to Vehicle	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Vehicle to Registration	Hierarchical Association
Link From Suspicious Activity to Vessel	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Aircraft	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ActivityLocationAssociation

Link Between Associated Components	Target Element
Link From Location to Location Coordinates	Hierarchical Association
Link From Location to Location Address	Hierarchical Association
Link From Suspicious Activity Report to Related ISE-SAR	Hierarchical Association
Link From Person to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonLocationAssociation
Link From Person to Contact Information	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityEmailAssociation or lexs:Digest/lexsdigest:Associations/lexsdigest:EntityTelephoneNumberAssociation
Link From Person to Driver License	Hierarchical Association
Link From Person to Passport	Hierarchical Association
Link From Person to Other Identifier	Hierarchical Association
Link From Person to Physical Descriptors	Hierarchical Association
Link From Person to Physical Feature	Hierarchical Association
Link From Person to Person Name	Hierarchical Association
Link From Suspicious Activity Report to Follow-Up Action	Hierarchical Association
Link From Target to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ItemLocationAssociation
Link From Suspicious Activity Report to Organization	Hierarchical Association
Link From Suspicious Activity to Person [Witness]	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentWitnessAssociation
Link From Suspicious Activity to Person [Person Of Interest]	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonOfInterestAssociation
Link From Organization to Target	ext:SuspiciousActivityReport/nc:OrganizationItemAssociation
Link from ISE-SAR Submission to Submitting Organization	Hierarchical Association
Link From Submitting Organization to Contact Information	Hierarchical Association (Note that the mapping indicates context and we are not reusing Contact Information components)

C. Extended XML Elements

Additional data elements are also identified as new elements outside of NIEM, Version 2.0. These elements are listed below:

AdditionalDetailsIndicator: Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.

AssignedByText: Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations.

AssignedToText: Text describing the person or sub-organization that will be performing the designated follow-up action.

ClassificationReasonText: A reason why the classification was made as such.

CriticalInfrastructureIndicator: Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

PrivacyFieldIndicator: Data element that may be used to identify an individual and therefore is subject to protection from disclosure under applicable privacy rules. Removal of privacy fields from a detailed report will result in a summary report. This privacy field informs users of the summary information exchange that additional information may be available from the originator of the report.

ReportPurgeDate: The date by which the privacy fields will be purged from the record system; general observation data is retained. Purge policies vary from jurisdiction to jurisdiction and should be indicated as part of the guidelines.

ReportPurgeReviewDate: Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR record.

SECTION V – INFORMATION EXCHANGE IMPLEMENTATION ARTIFACTS

A. Domain Model

1. General Domain Model Overview

The domain model provides a visual representation of the business data requirements and relationships (Figure 3). This Unified Modeling Language (UML)-based Model represents the Exchange Model artifact required in the information exchange development methodology. The model is designed to demonstrate the organization of data elements and illustrate how these elements are grouped together into Classes. Furthermore, it describes relationships between these Classes. A key consideration in the development of a Domain Model is that it must be independent of the mechanism intended to implement the model. The domain model is actually a representation of how data is structured from a *business* context. As the technology changes and new functional standards emerge, developers can create new standards mapping documents and schema tied to a new standard without having to re-address business process requirements.

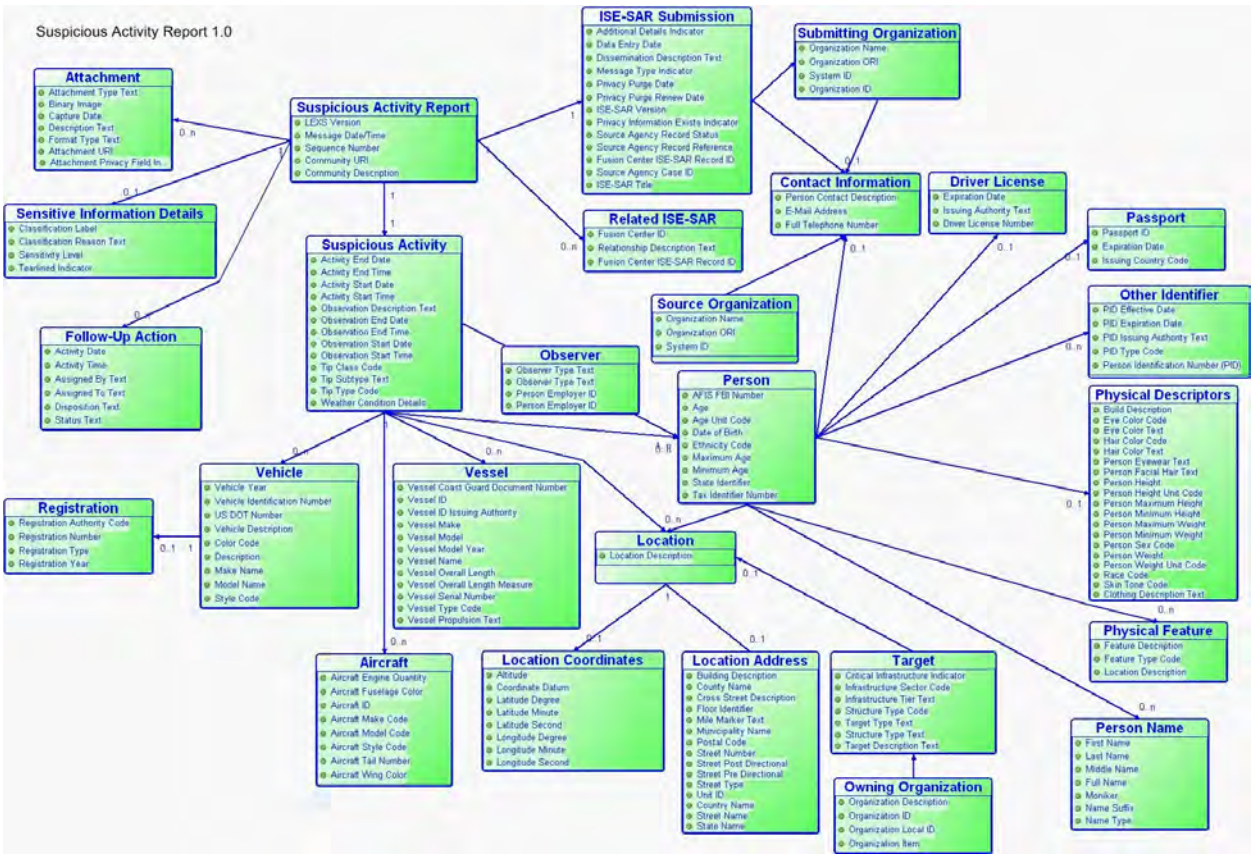


Figure 3 – UML-based Model[6]

B. General Mapping Overview

The detailed component mapping template provides a mechanism to cross-reference the business data requirements documented in the Domain Model to their corresponding XML Element in the XML Schema. It includes a number of items to help establish equivalency including the business definition and the corresponding XML Element Definition.

C. ISE-SAR Mapping Overview

The Mapping Spreadsheet contains seven unique items for each ISE-SAR data class and element. The Mapping Spreadsheet columns are described in this section.

[6] This figure may be also found in the technical artifacts folder that is part of this functional standard.

Table 4 – Mapping Spreadsheet Column Descriptions

Spreadsheet Name & Row	Description
Privacy Field Indicator	This field indicates that the information may be used to identify an individual.
Source Class/ Element	Content in this column is either the data class (grouping of data elements) or the actual data elements. Classes are highlighted and denoted with cells that contain blue background while elements have a white background. The word “Source” is referring to the ISE-SAR information exchange.
Source Definition	The content in this column is the class or element definition defined for this ISE-SAR information exchange. The word “Source” is referring to the ISE-SAR information exchange definition.
Target Element	The content in this column is the actual namespace path deemed equal to the related ISE-SAR information exchange element.
Target Element Definition	The content in this column provides the definition of the target or NIEM element located at the aforementioned source path. “Target” is referring to the NIEM definition.
Target Element Base	Indicates the data type of the terminal element. Data types of niem-xsd:String or nc:TextType indicate free-form text fields.
Mapping Comments	Provides technical implementation information for developers and implementers of the information exchange.

D. Schemas

The ISE-SAR Functional Standard contains the following compliant schemas;

- Subset Schema
- Exchange Schema
- Extension Schema
- Wantlist

E. Examples

The ISE-SAR Functional Standard contains two samples that illustrate exchange content as listed below.

1. XSL Style Sheet

This information exchange artifact provides an implementer and users with a communication tool which captures the look and feel of a familiar form, screen, or like peripheral medium for schema translation testing and user validation of business rules.

2. XML Instance

This information exchange artifact provides an actual payload of information with data content defined by the schema(s).

This page intentionally blank.

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
Eliciting Information	Questioning facility personnel about facility/infrastructure/personnel; this includes individuals probing employees in person on or off-site, over the phone, or via the Internet about particular structures, functions, and personnel procedures at the facility/infrastructure.
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Photography	Taking pictures/video of facility/infrastructure/personnel or surrounding environment.
Observation	Showing unusual interest in facility/infrastructure/personnel; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.
Surveillance	Monitoring the activity of people, facilities, processes or systems.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).
Sabotage/Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Testing of Security	Interactions with, or challenges to installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Flyover	Suspected over flight of a facility/infrastructure; this includes any type of flying vehicle (e.g., airplanes, helicopters, unmanned aerial vehicles, hang gliders).
Materials Acquisition/Storage	Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, timers), unauthorized/unlicensed individual/group attempts to obtain precursor chemicals/agents, or toxic materials, and rental of storage units for the purpose of storing chemicals or mixing apparatus.
Acquisition Of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other, unusual, capabilities, such as specialized transport or handling capabilities.
Weapons Discovery	Discovery of weapons or explosives.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data.
Other	Incidents not fitting any of the above categories.

This page intentionally blank.

PART C – ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The process begins when a person or persons observe unusual behavior. Such activities could include, but are not limited to, surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other usual behavior or sector-specific incidents.[7]	The observer may be a private citizen, a government official, or a law enforcement officer.
2	Initial Response and Investigation	An official of a Federal, State, or local agency with jurisdiction responds to the reported observation.[8] This official gathers additional facts through personal observations, interviews, and other investigative activities. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of fact based systems to continue the investigation. These fact based systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of fact based systems and the information they may provide include: Department of Motor Vehicles provides drivers license and vehicle registration information; National Crime Information Center provides wants and warrants information, criminal history information and access to the Terrorist Screening Center and the terrorist watch list, and Violent Gang/Terrorism Organization File (VGTOF); and, Other Federal, State, and local systems can provide criminal checks within the immediate and surrounding jurisdictions. When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).	The event may be documented using a variety of reporting mechanisms and processes, including but not limited to, reports of investigation, event histories, field interviews (FI), citations, incident reports, and arrest reports. The record may be hard and/or soft copy and does not yet constitute an ISE-SAR.

7 Suspicious activity reporting (SAR) is an official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism.

8 If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

Step	Activity	Process	Notes
3	Local/Regional Processing	The agency processes and stores the information in the RMS following agency policies and procedures. The flow will vary depending on whether the reporting organization is a State or local agency or a field element of a Federal agency. State and local: Based on specific criteria or the nature of the activity observed, the State or local law enforcement components forward the information to the State or major urban area fusion center for further analysis. Federal: Federal field components collecting suspicious activity would forward their reports to the appropriate resident, district, or division office. This information—still only fact information—would be reported to field intelligence groups or headquarters elements through processes that vary from agency to agency. In addition to providing the fact information to its headquarters, the Federal field component would provide an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.	The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region whether collected by SLT or Federal field components.
4	Creation of an ISE-SAR	The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria may have a nexus to terrorism. Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (ISE-SAR Functional Standard). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.	Some of this information may be intelligence, which identifies trends and other terrorist related information and is derived from Federal agencies such as NCTC, DHS, and the FBI. For State, local, and tribal law enforcement, the ISE-SAR information, may be fact information or criminal intelligence and is handled in accordance with 28 CFR Part 23. It may be shared with State or Federal law enforcement personnel with the privacy field included.
5	ISE-SAR Sharing and Dissemination	In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and placed in the State or major urban area fusion center's Shared Space or otherwise made available to members of the ISE. The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters. The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis.	

Step	Activity	Process	Notes
6	Federal Headquarters (HQ) Processing	At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with ISE members. The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).	When a State or local originated ISE-SAR is in the Federal system, the rules of sharing are no longer governed by 28 CFR Part 23, but rather by appropriate Federal privacy laws and guidelines.
7	NCTC Analysis	When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources. NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure web site. The Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of State, local, and tribal entities and when appropriate private sector entities. ITACG is the mechanism that facilitates the sharing of counterterrorism information with SLT.	
8	NCTC Alerts, Warnings, Notifications	NCTC products[9], informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with SLT through the State or major urban area fusion centers. The sharing with SLT and private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and ITACG informed products to help develop geographic-specific risk assessments (GSRA) to facilitate regional counterterrorism efforts. The GSRA are shared with SLT organizations and the private sector as appropriate. The recipient of the GSRA may use the GSRA to develop information gathering priorities or requirements.	NCTC products form the foundation of informational needs and guide collection of additional information. NCTC products should be responsive to informational needs of State, local, and tribal entities.

[9] NCTC product include: Alerts, warnings, and notifications—identifying time sensitive or strategic threats; Situational awareness reports; and Strategic and foundational assessments of terrorist risks and threats to the United States and related intelligence information.

Step	Activity	Process	Notes
9	Focused Collection	The information has come full circle and the process begins again, informed by an NCTC or other Federal organization's product and the identified information needs of State, local and tribal entities and Federal field components.	

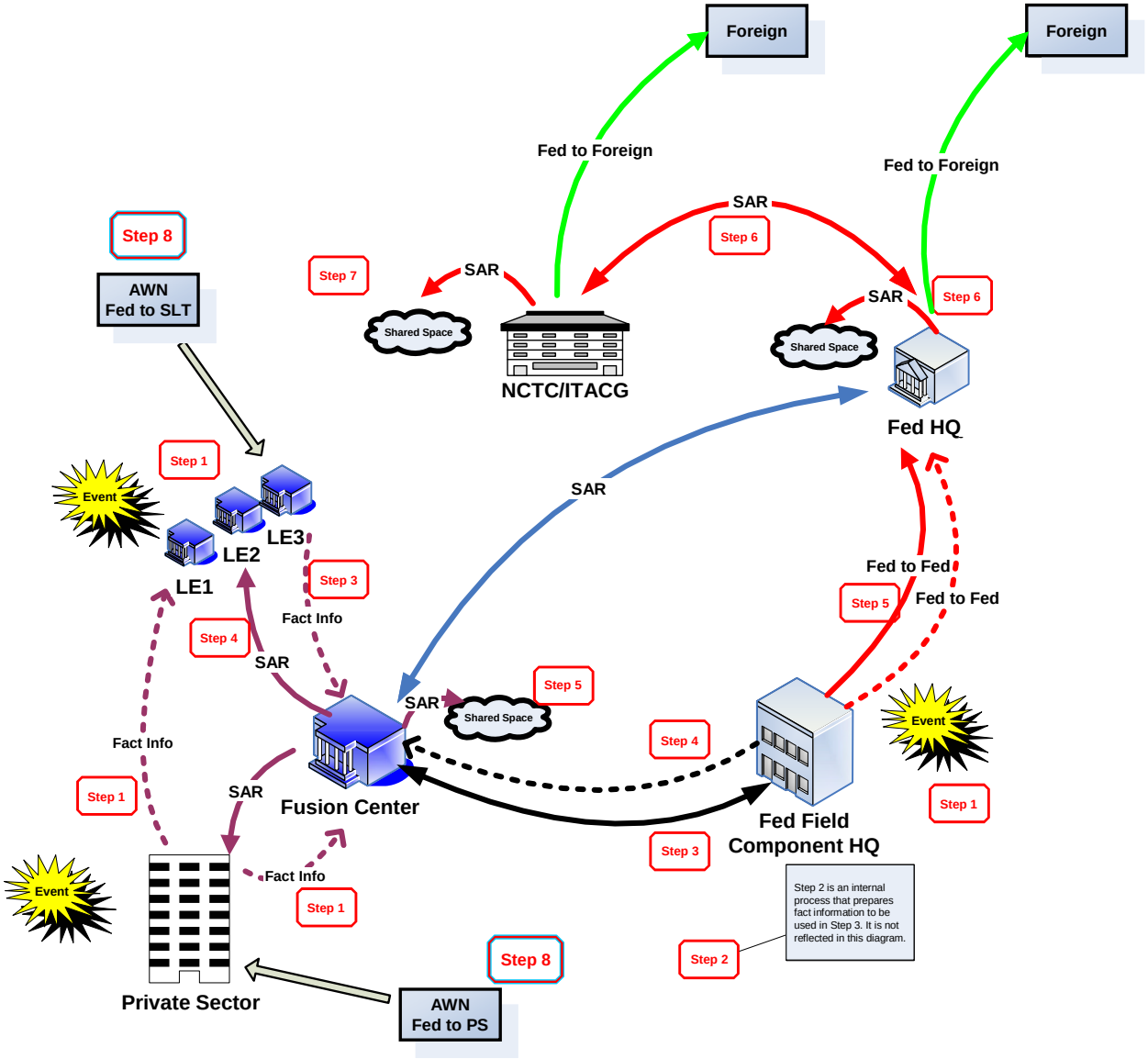


Figure 4 – SAR Information Flow Diagram