INFORMATION SHARING ENVIRONMENT (ISE)

FUNCTIONAL STANDARD (FS)

SUSPICIOUS ACTIVITY REPORTING (SAR)

VERSION 1.5

1. Authority. Homeland Security Act of 2002, 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, regulation, or policy.

2. Purpose. This issuance serves as the updated Functional Standard for ISE-SARs, and one of a series of Common Terrorism Information Sharing Standards (CTISS) issued by the PM-ISE. While limited to describing the ISE-SAR process and associated information exchanges, information from this process may support other ISE processes to include alerts, warnings, and notifications, situational awareness reporting, and terrorist watchlisting.

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, as specified in Section 1016(i) of the IRTPA.

4. References. ISE Implementation Plan, November 2006; ISE Enterprise Architecture Framework (EAF), Version 2.0, September 2008; Initial Privacy and Civil Liberties Analysis for the Information Sharing Environment, Version 1.0, September 2008; ISE-AM-300: Common Terrorism Information Standards Program, October 31, 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; Executive Order 13292 (Further Amendment to Executive Order 12958, as Amended, Classified National Security Information); Nationwide Suspicious Activity Reporting Concept of Operations, December 2008; ISE Suspicious Activity Reporting Evaluation Environment (EE) Segment Architecture, December 2008.

5. Definitions.

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

b. 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. CTISS, such as this *ISE-SAR Functional Standard*, are implemented in ISE participant infrastructures that include ISE Shared Spaces as described in the *ISE EAF*. Two categories of common standards are formally identified under CTISS:

   (1) Functional Standards – set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.

   (2) Technical Standards – document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.

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

d. ISE-Suspicious Activity Report (ISE-SAR): An ISE-SAR is a SAR (as defined below in 5i) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties 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. Personal Information: Information that may be used to identify an individual (i.e., data elements in the identified "privacy fields" of this *ISE-SAR Functional Standard*).

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

h. Suspicious Activity: Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

i. Suspicious Activity Report (SAR): Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

j. Universal Core (UCore): An interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of "who, what when, and where". UCore serves as a starting point for data level integration and permits the development of richer domain specific exchanges. UCore was developed in concert with NIEM program office, and is a collaborative effort between Department of Defense (DOD), DOJ, DHS and the Intelligence Community.

6. Guidance. This Functional Standard is hereby established as the nationwide ISE 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, civil rights, and civil liberties, 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 *ISE-SAR 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 organizations shall:

(1) Propose modifications 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 7.b (2) or 7.b (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 updated *ISE-SAR Functional Standard* until further updated, superseded, or cancelled.

Program Manager for the
Information Sharing Environment

Date: May 21, 2009

PART A – ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I – DOCUMENT OVERVIEW

A. List of ISE-SAR Functional Standard Technical Artifacts

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

Table 1 – Functional Standard Technical 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.
	5. Codified Data Field Values	Listings, descriptions, and sources as prescribed by data fields in the *ISE-SAR Functional Standard*.

[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, throughout the Information Sharing Environment (ISE), of information about suspicious activity, incidents, or behavior (hereafter collectively referred to as suspicious activity or activities) that have a potential terrorism nexus. The ISE includes 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. In addition to providing specific indications about possible terrorism-related crimes, ISE-SARs can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, State, or territory. Standardized and consistent sharing of suspicious activity information regarding criminal activity among State and major urban area fusion centers and Federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism. This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe potential criminal activity associated with terrorism and may be used by other communities to address other types of criminal activities where appropriate.

B. ISE-SAR Scope

Suspicious activity is defined as *observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.* A determination that such suspicious activity constitutes an ISE-SAR is made as part of a two-part process by trained analysts using explicit criteria. Some examples of the criteria for identifying those SARs, with defined relationships to criminal activity that also have a potential terrorism nexus, are listed below. Part B (ISE-SAR Criteria Guidance) provides a more thorough explanation of ISE-SAR criteria, highlighting the importance of context in interpreting such behaviors;

- Expressed or implied threat
- Theft/loss/diversion
- Site breach or physical intrusion
- Cyber attacks
- Probing of security response

[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.

It is important to stress that this *behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description). It is also important to recognize that many terrorism activities are now being funded via local or regional criminal organizations whose direct association with terrorism may be tenuous. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious activities or materials as a byproduct or secondary element in 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, there is value in sharing them more broadly to facilitate aggregate trending or analysis.

Suspicious Activity Reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory operations although they can provide information to these activities. The ISE-SAR effort offers a standardized means for sharing information regarding behavior potentially related to terrorism-related criminal activity and applying data analysis tools to the information. Any patterns identified during ISE-SAR data analysis may be investigated in cooperation with the reporting agency, Joint Terrorism Task Force (JTTF), or the State or major urban area fusion center in accordance with departmental policies and procedures. Moreover, the same constitutional standards that apply when conducting ordinary criminal investigations also apply to local law enforcement and homeland security officers conducting SAR inquiries. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop")[4], request identification, or detain and question an individual would apply in the same measure whether or not the observed behavior related to terrorism or any other criminal activity.

C. Overview of Nationwide SAR Cycle

As defined in the *Nationwide Suspicious Activity Reporting Initiative (NSI) Concept of Operations (CONOPS[5])* and shown in Figure 1, the nationwide SAR process involves a total of 12 discrete steps that are grouped under five standardized business process activities – Planning, Gathering and Processing, Analysis and Production, Dissemination, and Reevaluation. The top-level ISE-SAR business process described in this section has been revised to be consistent with the description in the *NSI CONOPS*. Consequently, the numbered steps in Figure 1 are the only ones that map directly to the nine-steps of the detailed information flow for nationwide SAR information sharing documented in Part C of this version of the *ISE-SAR Functional Standard*. For further detail on the 12 NSI steps, please refer to the *NSI CONOPS*.

---

4 "Terry Stop" refers to law enforcement circumstances related to Supreme Court of the United States ruling on "Terry v. Ohio (No. 67)" argued on December 12, 1967 and decided on June 10, 1968. This case allows a law enforcement officer to articulate reasonable suspicion as a result of a totality of circumstances (to include training and experience) and take action to frisk an individual for weapons that may endanger the officer. The Opinion of the Supreme Court regarding this case may be found at Internet site http://www.law.cornell.edu/supct/html/historics/USSC_CR_0392_0001_ZO.html.

5 PM-ISE, *Nationwide SAR Initiative Concept of Operations* (Washington: PM-ISE, 2008), available from www.ise.gov.

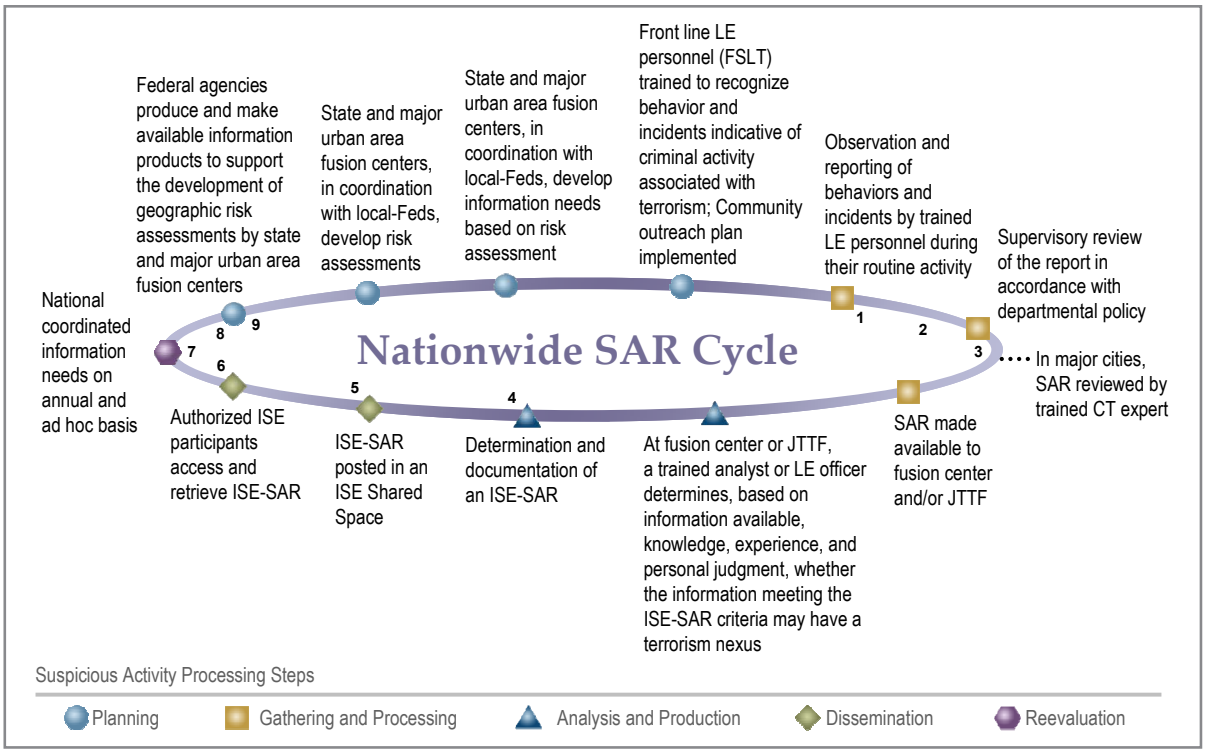

Figure 1. Overview of Nationwide SAR Process

D. ISE-SAR Top-Level Business Process

1. Planning

The activities in the planning phase of the NSI cycle, while integral to the overall NSI, are not discussed further in this Functional Standard. See the NSI CONOPS for more details.[6]

2. Gathering and Processing

Local law enforcement agencies or field elements of Federal agencies gather and document suspicious activity information in support of their responsibilities to investigate potential criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. Information acquisition begins with an observation or report of unusual or suspicious behavior that may be indicative of criminal activity associated with terrorism. Such activities include, but are not limited to, theft, loss, or diversion, site breach or physical intrusion, cyber attacks, possible testing of physical response, or other unusual behavior or sector specific incidents. It is important to emphasize that context is an essential element of interpreting the relevance of such behaviors to criminal activity associated with terrorism. (See Part B for more details.)

6 Ibid., 17-18.

Regardless of whether the initial observer is a private citizen, a representative of a private sector partner, a government official, or a law enforcement officer, suspicious activity is eventually reported to either a local law enforcement agency or a local, regional, or national office of a Federal agency. When the initial investigation or fact gathering is completed, the investigating official documents the event in accordance with agency policy, local ordinances, and State and Federal laws and regulations.

The information is reviewed within a local or Federal agency by appropriately designated officials for linkages to other suspicious or criminal activity in accordance with departmental policy and procedures.[7] Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to the State or major urban area fusion center or JTTF with minimal local processing. Major cities, on the other hand, may have trained counterterrorism experts on staff that apply a more rigorous analytic review of the initial reports and filter out those that can be determined not to have a potential terrorism nexus.

After appropriate local processing, agencies make SARs available to the relevant State or major urban area fusion center. Field components of Federal agencies forward their reports to the appropriate regional, district, or headquarters office employing processes that vary from agency to agency. Depending on the nature of the activity, the information could cross the threshold of "suspicious" and move immediately into law enforcement operations channels for follow-on action against the identified terrorist activity. In those cases where the local agency can determine that an activity has a direct connection to criminal activity associated with terrorism, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

3. Analysis and Production

The fusion center or Federal agency enters the SAR into its local information system and then performs an additional analytic review to establish or discount a potential terrorism nexus. First, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria outlined in Part B of this *ISE-SAR Functional Standard*. Second, the Terrorist Screening Center (TSC) should be contacted to determine if there is valuable information in the Terrorist Screening Database. Third, he or she will review the input against all available knowledge and information for linkages to other suspicious or criminal activity.

Based on this review, the officer or analyst will apply his or her professional judgment to determine whether the information has a potential nexus to terrorism. If the officer or analyst cannot make this explicit determination, the report will not be accessible by the ISE, although

[7] If appropriate, the agency may consult with a Joint Terrorism Task Force, Field Intelligence Group, or fusion center.

it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules.[8]

4. Dissemination

Once the determination of a potential terrorism nexus is made, the information becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Information Exchange Package Document (IEPD) format described in Sections III and IV. This ISE-SAR is then stored in the fusion center, JTTF, or other Federal agency's ISE Shared Space[9] where it can be accessed by authorized law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility as well as other ISE participants, including JTTFs. This allows the fusion center to be cognizant of all terrorist-related suspicious activity in its area of responsibility, consistent with the information flow description in Part C. Although the information in ISE Shared Spaces is accessible by other ISE participants, it remains under the control of the submitting organization, i.e., the fusion center or Federal agency that made the initial determination that the activity constituted an ISE-SAR.

By this stage of the process, all initially reported SARs have been through multiple levels of review by trained personnel and, to the maximum extent possible, those reports without a potential terrorism nexus have been filtered out. Those reports posted in ISE Shared Spaces, therefore, can be presumed by Federal, State, and local analytic personnel to be terrorism-related and information derived from them can be used along with other sources to support counterterrorism operations or develop counterterrorism analytic products. As in any analytic process, however, all information is subject to further review and validation, and analysts must coordinate with the submitting organization to ensure that the information is still valid and obtain any available relevant supplementary material before incorporating it into an analytic product.

Once ISE-SARs are accessible, they can be used to support a range of counterterrorism analytic and operational activities. This step involves the actions necessary to integrate ISE-SAR information into existing counterterrorism analytic and operational processes, including efforts to "connect the dots," identify information gaps, and develop formal analytic products. Depending on privacy policy and procedures established for the NSI as a whole or by agencies responsible for individual ISE Shared Spaces, requestors may only be able to view reports in the Summary ISE-SAR Information format, i.e., without privacy fields. In these cases, requestors should contact the submitting organization directly to discuss the particular report more fully and obtain access, where appropriate, to the information in the privacy fields.

---

[8] As was already noted in the discussion of processing by local agencies, where the fusion center or Federal agency can determine that an activity has a direct connection to a possible terrorism-related crime, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation.

[9] PM-ISE, *ISE Enterprise Architecture Framework, Version 2.0*, (Washington: PM-ISE, 2008), 61-63

5. Reevaluation[10]

Operational feedback on the status of ISE-SARs is an essential element of an effective NSI process with important implications for privacy and civil liberties. First of all, it is important to notify source organizations when information they provide is designated as an ISE-SAR by a submitting organization and made available for sharing—a form of positive feedback that lets organizations know that their initial suspicions have some validity. Moreover, the process must support notification of all ISE participants when further evidence determines that an ISE-SAR was designated incorrectly so that the original information does not continue to be used as the basis for analysis or action. This type of feedback can support organizational redress processes and procedures where appropriate.

E. Broader ISE-SAR Applicability

Consistent with the 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 sensitive but unclassified (SBU)/controlled unclassified information (CUI) within the ISE. There is also a provision for using a data element indicator for designating classified national security information as part of the ISE-SAR record, as necessary. This condition could be required under special circumstances for protecting the context of the event, or specifics or organizational associations of affected locations. The State or major urban area fusion center shall act as the key conduit between the State, local, and tribal (SLT) agencies and other ISE participants. It is also important to note that the ISE Shared Spaces implementation concept is focused exclusively on terrorism-related information. However many SAR originators and consumers have responsibilities beyond terrorist activities. Of special note, there is no intention to modify or otherwise affect, through this *ISE-SAR Functional Standard*, the currently supported or mandated direct interactions between State, local, and tribal law enforcement and investigatory personnel and the Joint Terrorism Task Forces (JTTFs) or Field Intelligence Groups (FIGs).

This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all ISE participants. Although the extensibility of this *ISE-SAR Functional Standard* does support customization for unique communities, jurisdictions planning to modify this *ISE-SAR Functional Standard* must carefully consider the consequences of customization. The PM-ISE requests that modification follow a formal change request process through the ISE-SAR Steering Committee 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.

[10] The Reevaluation Phase also encompasses the establishment of an integrated counterterrorism information needs process, a process that does not relate directly to information exchanges through this standard. See page 23 of the *NSI CONOPS* for more details.

F. Protecting Privacy

Laws that prohibit or otherwise limit the sharing of personal information vary considerably between the Federal, State, local, and tribal 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 statutes and regulations, different State, local or tribal laws, regulations, or policies that affect privacy. One method for protecting privacy while enabling the broadest possible sharing is to anonymize ISE-SAR reports by excluding data elements that contain personal information. Accordingly, two different formats are available for ISE-SAR information. The **Detailed ISE-SAR IEPD** format includes personal information contained in the data fields set forth in Section IV of this *ISE-SAR Functional Standard* ("ISE-SAR Exchange Data Model"), including "privacy fields" denoted as containing personal information. If an ISE participant is not authorized to disseminate personal information from an ISE Shared Space (e.g., the requester site does not have a compliant privacy policy) or the SAR does not evidence the necessary nexus to terrorism-related crime (as required by this *ISE-SAR Functional Standard*), information from the privacy fields will not be loaded into the responsive document (search results) from the ISE Shared Space. This personal information will not be passed to the ISE participant. The **Summary ISE-SAR Information** format excludes privacy fields or data elements identified in Section IV of this *ISE-SAR Functional Standard* as containing personal information. Each ISE participant can exclude additional data elements from the **Summary ISE-SAR Information** format in accordance with its own legal and policy requirements. It is believed the data contained within a **Summary ISE-SAR Information** format will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the sending organization. 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*.

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 IEPD**.

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 ISE-SAR IEPD** or **Summary ISE-SAR Information**. The basic ISE-SAR information exchange is documented using five unique artifacts giving implementers tangible products that 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. Fifth, a codified data field values listing provides listings, descriptions, and sources as prescribed by the data fields.

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 community through their ISE Shared Space. 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 Wing Color	A code identifying a color of a wing of an aircraft.
X	Aircraft ID	A unique identifier assigned to the aircraft by the observing organization—used for referencing. *If this identifier can be used to identify a specific aircraft, for instance, by using the aircraft tail number, then this element is a privacy field. [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.

Privacy Field	Source Class/Element	Source Definition
	Aircraft Style Code	A code identifying a style of an aircraft.
X	Aircraft Tail Number	An aircraft identification number prominently displayed at various locations on an aircraft, such as on the tail and along the fuselage. [free text field]
	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	
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year 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 the observer or 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	

Privacy Field	Source Class/Element	Source Definition
X	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]
	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]
	ICAO Airfield Code for Departure	An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information. [free text field]
	ICAO Airfield Code for Planned Destination	An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information [free text field]
	ICAO for Actual Destination	An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	ICAO Airfield for Alternate	An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [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]
X	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]
X	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).

Privacy Field	Source Class/Element	Source Definition
	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).
	Conveyance track/intent	A direction by heading and speed or enroute route and/or waypoint of conveyance [free text field]
	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	
	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]
X	PID Effective Date	The month, date, and year that the PID number became active or accurate.
	PID Effective Year	The year that the PID number became active or accurate.
X	PID Expiration Date	The month, date, and year that the PID number expires.
	PID Expiration Year	The year 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]
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year 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]

Privacy Field	Source Class/Element	Source Definition
	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]
X	Date of Birth	The month, date, and year that a person was born.
	Year of Birth	The year 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]
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.

Privacy Field	Source Class/Element	Source Definition
	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, tattoos, 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	
	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 registration 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 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).

Privacy Field	Source Class/Element	Source Definition
	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 IEPD 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 Submission Date	Date of submission for the ISE-SAR Record.
	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 Code	The current status of the record within the source agency system.
	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]
	Fusion Center Submission Date	Date of submission to the Fusion Center.
	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]

Privacy Field	Source Class/Element	Source Definition
	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.
	Source Reliability Code	Reliability of the source, in the assessment of the reporting organization: could be one of ‘reliable’, ‘unreliable’, or ‘unknown’
	Content Validity Code	Validity of the content, in the assessment of the reporting organization: could be one of ‘confirmed’, ‘doubtful’, or ‘cannot be judged’
	Nature of Source-Code	Nature of the source: Could be one of ‘anonymous tip’, ‘confidential source’, trained interviewer’, ‘written statement – victim, witness, other’, private sector’, or ‘other source’
	Nature of Source-Text	Optional information of ‘other source’ is selected above. [free text field]
	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]
	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.

Privacy Field	Source Class/Element	Source Definition
	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.
	Threat Type Code	Broad category of threat to which the tip or lead pertains. Includes Financial Incident, Suspicious Activity, and Cyber Crime.
	Threat Type Detail 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]
	Suspicious Activity 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.
	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.

Privacy Field	Source Class/Element	Source Definition
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 Official Coast Guard Number Identification	An identification for the Official (U.S. Coast Guard Number of a vessel). 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]
	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]
X	Vessel IMO Number Identification	An identification for an International Maritime Organization Number (IMO number) of a vessel [free text field]
	Vessel MMSI Identification	An identification for the Maritime Mobile Service Identity (MMSI) or a vessel [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 Hailing Port	The identifying attributes of the hailing port of a vessel [free text field]
	Vessel National Flag	A data concept for a country under which a vessel sails. [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.

Privacy Field	Source Class/Element	Source Definition
	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 2 (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 From Suspicious Activity to Target	Hierarchical Association
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 Between Associated Components	Target Element
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.

ContentValidityCode: Validity of the content, in the assessment of the reporting organization: could be one of ‘confirmed’, ‘doubtful’, or ‘cannot be judged’.

Conveyancetrack/intent: A direction by heading and speed or enroute route and/or waypoint of conveyance.

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.

ICAOAirfieldCodeforDeparture: An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information.

ICAOAirfieldCodeforPlannedDestination: An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOforActualDestination: An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOAirfieldforAlternate: An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

NatureofSource-Code: Nature of the source: Could be one of ‘anonymous tip’, ‘confidential source’, trained interviewer’, ‘written statement – victim, witness, other’, private sector’, or ‘other source’.

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 IEPD record.

SourceReliabilityCode: Reliability of the source, in the assessment of the reporting organization: could be one of ‘reliable’, ‘unreliable’, or ‘unknown’.

VesselHailingPort: The identifying attributes of the hailing port of a vessel.

VesselNationalFlag: A data concept for a country under which a vessel sails.

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 2). 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.

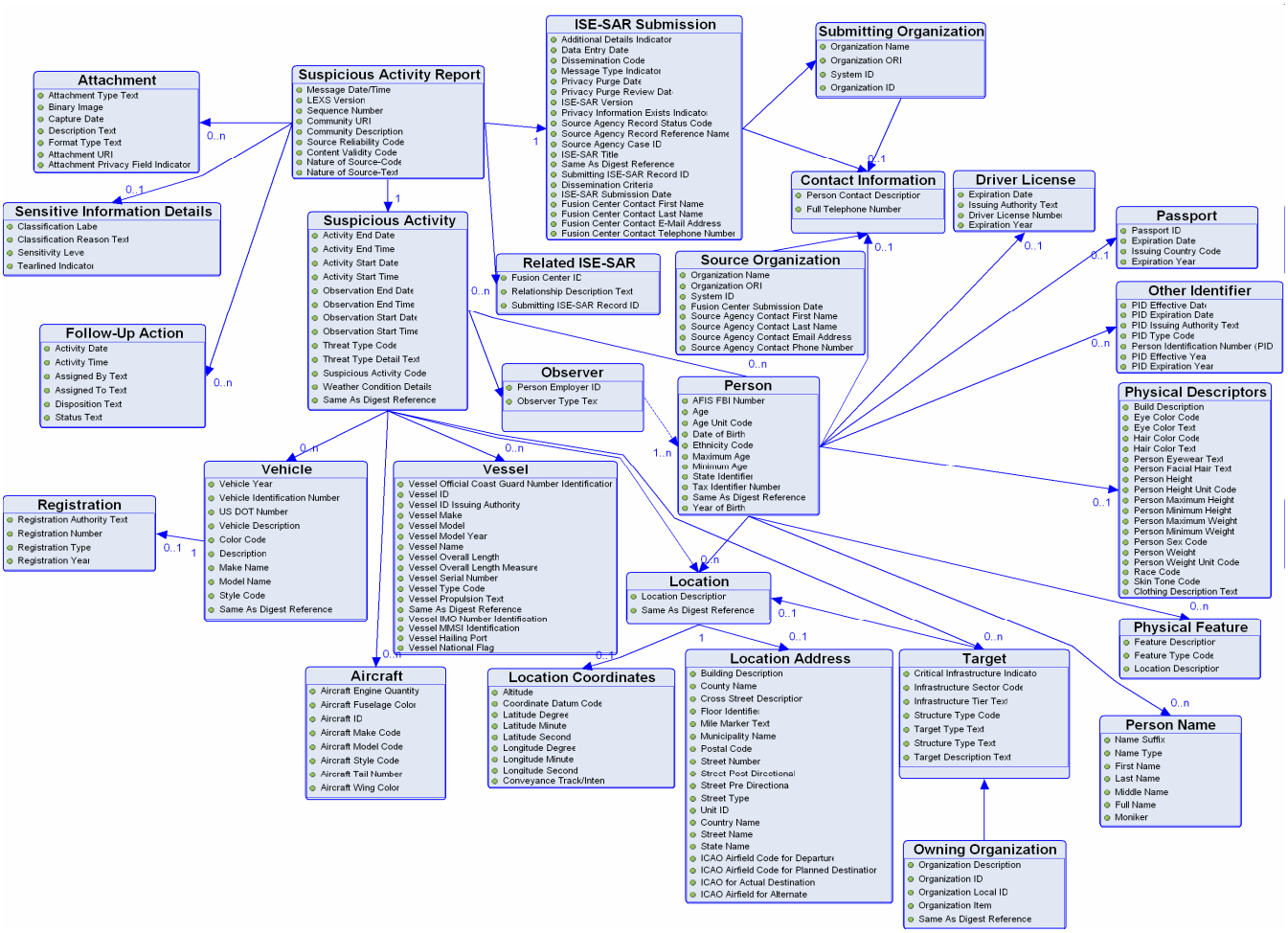

Figure 2 – UML-based Model

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.

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).

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
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.
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.
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.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION[11]	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

[11] Note: These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may used as specific suspect descriptions).

Category	Description
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
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.

PART C – ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The information flow begins when a person observes behavior or activities that would appear suspicious to a reasonable person. Such activities could include, but are not limited to, expressed or implied threats, probing of security responses, site breach or physical intrusion, cyber attacks, 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.[12]	The observer may be a private citizen, a government official, or a law enforcement officer.

[12] Suspicious activity reporting (SAR) is official documentation of observed behavior that may be reasonably indicative of intelligence gathering and/or pre-operational planning related to terrorism or other criminal activity. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Step	Activity	Process	Notes
2	Initial Response and Investigation	An official of a Federal, State, local, or tribal agency with jurisdiction responds to the reported observation.[13] This official gathers additional facts through personal observations, interviews, and other investigative activities. This may, at the discretion of the official, require further observation or engaging the subject in conversation. Additional information acquired from such limited investigative activity could then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process. 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 information systems to continue the investigation. These systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of such 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, Violent Gang/Terrorism Organization File (VGTOF), and Regional Information Sharing System (RISS); Other Federal, State, local, and tribal 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.

[13] 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, local, and tribal: Based on specific criteria or the nature of the activity observed, the State, local, and tribal 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 would be reported to field intelligence groups or headquarters elements through processes that vary from agency to agency. In addition to providing the 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 State, local, or tribal entities, 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 behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential 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 used to develop criminal intelligence information or intelligence products which identifies trends and other terrorism 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 or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23.

Step	Activity	Process	Notes
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 ISE 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.	
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).	
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 State, local, and tribal entities.	

Step	Activity	Process	Notes
8	NCTC Alerts, Warnings, Notifications	NCTC products[14], informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with State, local, and tribal entities through the State or major urban area fusion centers. The sharing with State, local, and tribal entities 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 State, local, and tribal entities 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	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.	

[14] 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.

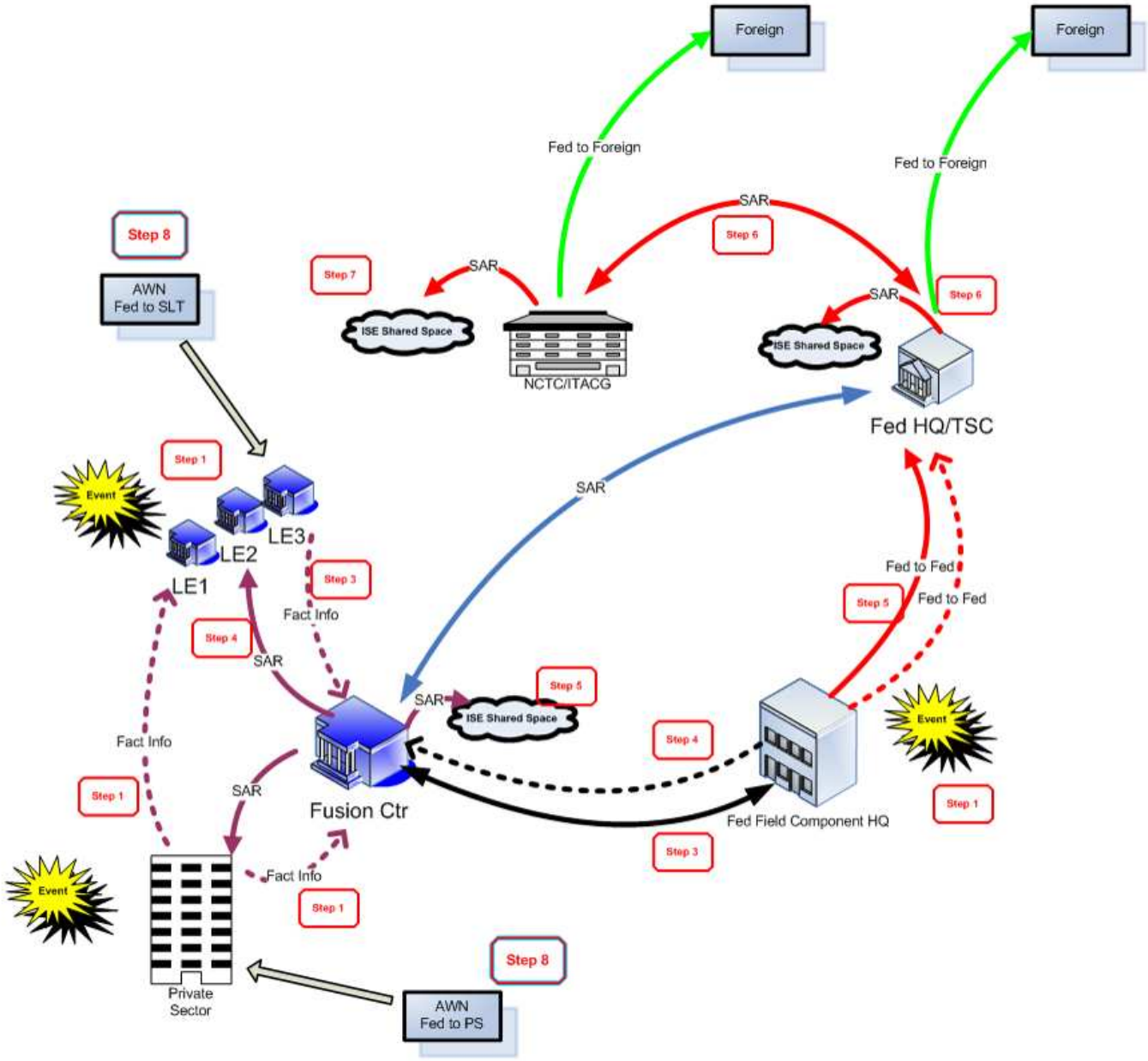

Figure 3 – SAR Information Flow Diagram