Archived Content

In an effort to keep DHS.gov current, this document has been archived and contains outdated information that may not reflect current policy or programs.

INFORMATION SHARING ENVIRONMENT (ISE)

FUNCTIONAL STANDARD (FS)

SUSPICIOUS ACTIVITY REPORTING (SAR)

VERSION 1.5.5

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 updates the Functional Standard for ISE-SARs and is one of a series of Common Terrorism Information Sharing Standards (CTISS) issued by the Program Manager for the Information Sharing Environment (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-SAR Functional Standard* applies to all departments or agencies that possess or use terrorism or homeland security information or intelligence, 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, and in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).

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; Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations, Nationwide Suspicious Activity Reporting Initiative (July 2010); 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 (CONOPS), Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23; Executive Order 13526 (Classified National Security Information), December 29, 2009; Nationwide Suspicious Activity Reporting Concept of Operations, December 2008; ISE Suspicious Activity Reporting Evaluation Environment (EE) Segment Architecture, December 2008; *ISE-SAR Functional Standard* v. 1.5 (2009); and the National Strategy for Information Sharing and Safeguarding, December 2012; NSI SAR Data Repository (SDR) CONOPS, January 2014.

5. Definitions.

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

b. Common Terrorism Information Sharing Standards (CTISS): Business process-driven, performance-based "common standards" for preparing terrorism-related (and other) information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism-related information within the ISE. CTISS, such as this *ISE-SAR Functional Standard*, are implemented in ISE participants' infrastructures as described in the *ISE EAF*. CTISS identifies two categories of common standards:

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. Nationwide SAR Initiative (NSI) SAR Data Repository (SDR): The NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, which incorporates Federal, State, and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.

d. eGuardian: eGuardian is the FBI's unclassified, Web-based system for receiving, tracking, and sharing ISE-SARs in the NSI as well as receiving and documenting other terrorism-related information, such as watchlist encounters or terrorism-related events, and other cyber or criminal threat information. (All information that is available to NSI participants through the eGuardian SDR will be vetted by a trained fusion center or Federal agency analyst or investigator to ensure that it meets the vetting standard for an ISE-SAR (i.e., a SAR that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism). ISE-SARs loaded into eGuardian are pushed to the FBI's Guardian system, a classified counterpart to eGuardian, in which the FBI and its JTTFs compare investigative lead information with other holdings available to the FBI in its capacity as a member of the Intelligence Community.

e. Field Intelligence Groups (FIGs): The hub of the FBI's intelligence program in the field, FIGs are the primary mechanism through which FBI field offices identify, evaluate, and prioritize threats within their territories. Using dissemination protocols, FIGs contribute to regional and local perspectives on threats and serve as the FBI's link among fusion centers, the JTTFs, and the Intelligence Community.

f. Fusion center: "A collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent,

investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal government and SLTT and private-sector partners.

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

h. Information Sharing Environment-Suspicious Activity Report (ISE-SAR): An ISE-SAR is a SAR (as defined below in 5.t) that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business rules and privacy and civil liberties requirements will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

i. Joint Terrorism Task Forces (JTTFs): The FBI's JTTFs are interagency task forces designed to enhance communication, coordination, and cooperation in countering terrorist threats. They combine the resources, talents, skills, and knowledge of Federal, State, territorial, tribal, and local law enforcement and homeland security agencies, as well as the Intelligence Community, into a single team that investigates and/or responds to terrorist threats. The JTTFs execute the FBI's lead Federal agency responsibility for investigating terrorist acts or terrorist threats against the United States.

j. 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.

k. Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI): The NSI establishes standardized processes and policies that provide the capability for Federal, SLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant ISE-SARs through a distributed information sharing system that protects privacy, civil rights, and civil liberties.

l. Owning agency/organization: The organization that owns the target associated with the suspicious activity.

m. Personally identifiable 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*).

n. Pre-operational planning: Pre-operational planning describes activities associated with a known or particular planned criminal operation or with terrorist operations generally.

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

p. Reasonably indicative: This operational concept for documenting and sharing suspicious activity report takes into account the circumstances in which that observation is made, which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate pre-operational planning associated with terrorism or other criminal activity.[1] It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

q. Source agency/organization: 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.

r. Submitting agency/organization: The organization that actuates the push of the ISE-SAR to the NSI community. The submitting organization and the source organization may be the same.

s. Suspicious activity: Observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.

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

6. Guidance. This Functional Standard is hereby established as the nationwide ISE Functional Standard for identifying 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 agencies participating in the NSI.

7. Responsibilities.

a. The PM-ISE, in consultation with the Information Sharing and Access Interagency Policy Committee (ISA IPC), will:

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

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

[1] It should be noted that for purposes of the evaluation and documentation of an ISE-SAR (See 5. h., above), the term "other criminal activity" must refer to criminal activity associated with terrorism and must fall within the scope of the 16 terrorism pre-operational behaviors identified in Part B of this Functional Standard.

(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, training, and governance structure, as appropriate, to address privacy, civil rights, and civil liberties-related policy, architecture, and legal issues.

(4) Work with ISE agencies participating in the NSI, through the ISA IPC governance process, to develop a new or modified *ISE-SAR Functional Standard*, as needed and recognize the separate process for DHS and the FBI to update the behavioral examples in Part B ISE-SAR Criteria Guidance to rapidly reflect emerging threats and trends.

(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 ISA IPC 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 that 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 ISA IPC Privacy and Civil Liberties Subcommittee (P/CL Subcommittee).

(5) Ensure that incorporation of this ISE-SAR Functional Standard, as set forth in 7.b (1) or 7.b (2) above, is done without impact on federal agencies' lawful collection, maintenance, dissemination, and use of information, as provided by federal law.

8. Effective Date and Expiration. This *ISE-SAR Functional Standard* supersedes the Information Sharing Environment, Functional Standard, Suspicious Activity Reporting, v. 1.5 (2009), 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: February 23, 2015

Document Change History	
Document Title	**ISE-SAR Functional Standard**
Document Owner	**PM-ISE**
Document Responsibility	**PM-ISE**
Document Version	**1.5.5**
Document Status	

Version Control Summary			
Date	**Version**	**Changed by**	**Change Description**
2/23/15	1.5.5		Update to version 1.5 promulgated

Future Releases		
Date	**Version**	**Proposed**

PART A—ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I: DOCUMENT OVERVIEW

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[2]

Artifact Type	Artifact	Artifact Description
Development and Implementation Tools	1. Component Mapping Template (CMT) (SAR-to-NIEM)	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 NIEM 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*.

[2] Development and implementation tools may be accessible through www.ise.gov. In addition, updated versions of this Functional Standard should conform with NIEM.

SECTION II: SUSPICIOUS ACTIVITY REPORTING EXCHANGES

A. ISE-SAR Purpose

This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe pre-operational behaviors that are criminal in nature and have historically been associated with terrorism.[3] The NSI includes law enforcement,[4] homeland security,[5] and other information sharing partners at the Federal, SLTT levels, including State and major urban area fusion centers, to the full extent permitted by law. In addition to providing specific indications about possible terrorism-related behaviors, 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, including SLTT jurisdictions. Standardized and consistent sharing of ISE-SARs among State and major urban area fusion centers and Federal agencies participating in the NSI is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe pre-operational behaviors historically associated with terrorism.

B. ISE-SAR Scope

An ISE-SAR is a SAR that has been determined by a trained analyst or investigator, pursuant to a two-part process,[6] to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). (See Section II. D. 3. below, Analysis and Production). "Reasonably indicative" is a determination that takes into account (1) the circumstances in which the observation is made, which creates in the mind of the reasonable observer an articulable concern that the behavior may indicate pre-operational planning associated with terrorism or other criminal activity; and (2) the training and expertise of a reasonable law enforcement officer, in cases in which an officer is the observer or documenter of the SAR, who may be informed by specific or general threat bulletins, trip wire reports, or other information or intelligence. The term "pre-operational planning" refers to those activities that are associated with a known or particular planned criminal operation or with terrorist operations generally.

---

[3] Identified in Part B of this Functional Standard, the 16 pre-operational behaviors are criminal in nature either because they are inherently criminal (e.g., breach, theft, sabotage) or because they are being engaged in to further a terrorism operation (e.g., testing or probing of security, observation/surveillance, materials acquisition). The pre-operational behavioral criteria and categories are listed in Part B of this Functional Standard.

[4] All references to Federal and SLTT law enforcement agencies are intended to encompass civilian law enforcement, military police, and other security professionals.

[5] 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.

[6] The determination of an ISE-SAR is a two-part process: (1) at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information for suspicious behavior based on his or her training and expertise and against ISE-SAR behavior criteria; and (2) based on the context, facts, and circumstances, the analyst or investigator determines whether the information meeting the criteria has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).

A determination that a SAR constitutes an ISE-SAR is made as part of a two-part vetting process by a trained analyst or investigator who takes into account the reported circumstances of the SAR, including both the training and experience of the law enforcement or homeland security personnel reporting the behavior, to confirm that the reasonably indicative determination has been met.[7] The analyst or investigator then compares the SAR with information from available databases and resources, reviews the behavior against the Part B (ISE-SAR Criteria Guidance) pre-operational terrorism behaviors, and then makes a judgment as to whether, given the context, facts, and circumstances available, there is a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). Part B provides a more thorough explanation of ISE-SAR pre-operational behavior criteria and highlights the importance of the trained analyst or investigator taking into account the context, facts, and circumstances in reviewing suspicious behaviors to identify those SARs with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). The following are select examples of the 16 terrorism pre-operational behavioral categories, set forth in Part B, that may be reasonably indicative of terrorism:

Expressed or implied threat

Theft/loss/diversion

Breach/attempted intrusion

Cyberattacks

Testing or probing of security[8]

It is important to stress that this *behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).[9] The same constitutional standards that apply when conducting ordinary criminal investigations also apply to Federal and SLTT law enforcement and homeland security officers collecting information about suspicious activity. The ISE-SAR Functional Standard does not alter law enforcement officers' constitutional obligations when interacting with the public. This means, for example, that constitutional protections and agency policies and procedures that apply to a law

[7] In assessing whether behavior constitutes "suspicious activity," law enforcement and homeland security personnel should consider all of the circumstances in which the behavior was observed, including knowledge such personnel may have had of any emerging threats or tradecraft, such as those based on specific or general threat bulletins, trip wire reports, or other information or intelligence.

[8] For a full list and explanation of the behavioral categories, behavioral criteria, and descriptive examples, see Part B.

[9] Consideration and documentation of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity shall be consistent with applicable guidance, including, for federal law enforcement officers, *Guidance for Federal Law Enforcement Agencies regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (December 2014).

enforcement officer's authority to stop, stop and frisk ("Terry Stop")[10], request identification, or detain and question an individual apply in the same measure to observed behavior that is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. It is also important to recognize that many terrorism-related 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 behaviors as a by-product or secondary element in a criminal enforcement or investigative activity. This means that, while some ISE-SARs may document observed behaviors to which local agencies have already responded, there is value in sharing them more broadly to facilitate aggregate trending or analysis of potential terrorist activities.

ISE-SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory operations, although they can provide information on these activities. The ISE-SAR process offers a standardized means for identifying and sharing ISE-SARs and applying data analytic tools to the information. Any patterns identified during ISE-SAR data analysis must be investigated in cooperation with the FBI's JTTFs. If the information originates with the JTTF, the JTTF should work in coordination with the State or major urban area fusion center unless departmental policies and procedures dictate otherwise (e.g., the information is classified).

C. Overview of Nationwide SAR Cycle

As defined in the *Nationwide Suspicious Activity Reporting Initiative (NSI) Concept of Operations (CONOPS),*[11] the Nationwide SAR process consists of five standardized business process categories: (1) planning; (2) gathering and processing; (3)analysis and production; (4) dissemination; and (4) reevaluation. Under these five categories are nine steps that complete the Nationwide SAR cycle, as illustrated below in Figure 1. Figure 1 relates to the detailed ISE-SAR flowchart outlined 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.*

[10] "Terry Stop" refers to the U.S. Supreme Court ruling in *Terry v. Ohio*, 392 U.S. 1 (1968), which held that a law enforcement officer may stop and frisk an individual for weapons that may endanger the officer when the officer has a reasonable and articulable suspicion, based on a totality of the circumstances, that the individual may be armed and dangerous.

[11] PM-ISE, *Nationwide SAR Initiative Concept of Operations* (2008), available from http://ise.gov/sites/default/files/NSI_CONOPS_Version_1_FINAL_2008-12-11_r1.0.pdf.

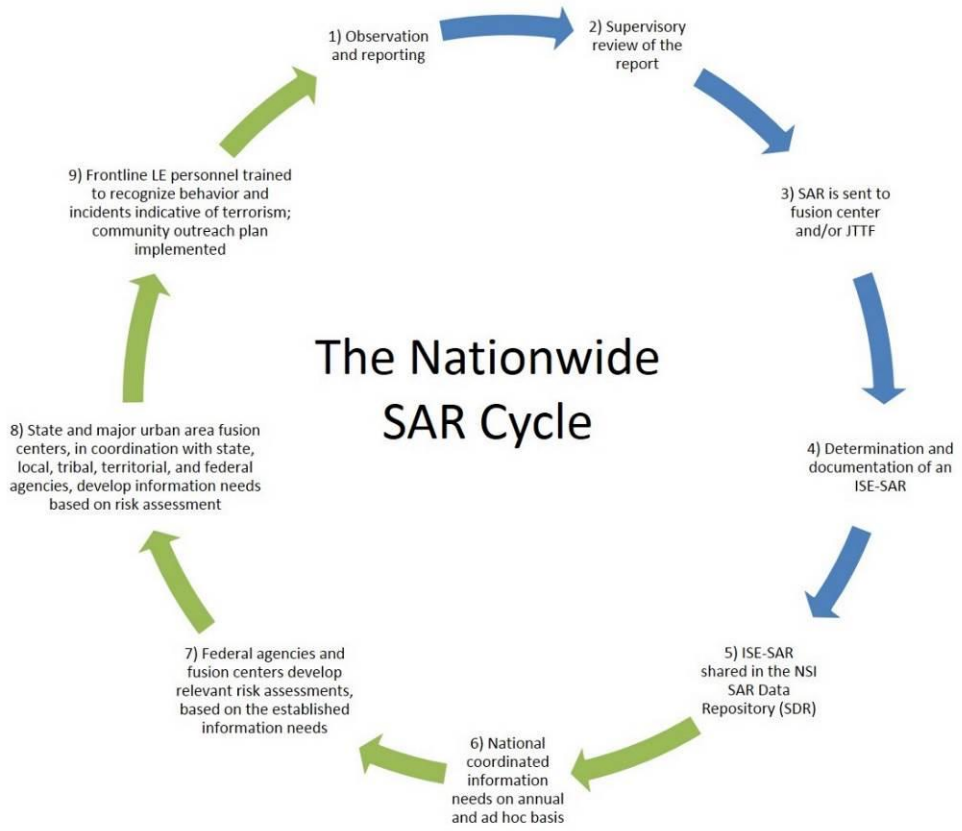

Figure 1 – ISE-SAR Flowchart

The technical framework of the SAR vetting and approval process that may produce an ISE-SAR is discussed in the *Nationwide Suspicious Activity Reporting (SAR) Initiative SAR Data Repository (SDR) Concept of Operations* (NSI SDR CONOPS).[12] The NSI SDR CONOPS explains the technical solution and associated user and training requirements supporting the NSI and details the enhanced platform that offers new efficiencies and deploys distributed capabilities to the NSI user community. The NSI SDR CONOPS provides an overview of the rules, regulations, policies, and training associated with accessing, submitting, and searching SAR data residing in the NSI SDR and the various tools that enable those submissions and searches.

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.

[12] The NSI SDR CONOPS, (2014), available from https://leo.cjis.gov/leoContent/docs/gen/lesig/e_guard/fbi_reports/2014/201401_nsi_sar_data_repository_conops.pdf.

2. Gathering and Processing

SLTT law enforcement agencies, homeland security agencies, or field elements of Federal agencies participating in the NSI gather, document, and report information about suspicious activity 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 which, under the circumstances, is reasonably indicative of pre-operational planning associated with terrorism or other criminal activity. Behaviors that may be reasonably indicative of pre-operational planning associated with terrorism include, but are not limited to, theft, loss, or diversion, site breach or physical intrusion, cyberattacks, possible testing of physical response, or other unusual behavior or sector-specific incidents. It is important to emphasize that context, facts, and circumstances are essential elements for determining the relevance of suspicious behaviors to criminal activity with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). (See Part B for more details.)

Regardless of whether the initial observer is a private citizen, a representative of a private-sector partner, a government official, or a law enforcement or homeland security officer, suspicious activity may be reported to an SLTT law enforcement agency, a fusion center, or a local, regional, or national office of a Federal agency. When the initial investigation or fact gathering is completed, the investigating officer or official documents the event as a SAR, in accordance with the *ISE-SAR Functional Standard*, agency policy, local ordinances, and State and Federal laws and regulations.

The SAR is then reviewed within an SLTT or Federal agency by appropriately designated supervisors or other officials, who may have operational, privacy, and civil liberties responsibilities, for linkages to other suspicious or criminal activity in accordance with agency or departmental policy and procedures.[13] Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to their State or major urban area fusion centers or their local FBI JTTF, where further analysis can take place to determine whether the SAR reflects a Part B terrorism pre-operational behavior, has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism), and is therefore an ISE-SAR. Major cities, on the other hand, may have trained counterterrorism experts on staff that perform analytic review of the initial reports and filter out those that can be determined not to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism).

After appropriate local processing, SLTT agencies make SARs available to their relevant State or major urban area fusion centers. Field components of Federal agencies participating in the NSI forward their SARs to the appropriate regional, district, or headquarters office, employing processes that vary from agency to agency. In those cases in which a local agency can determine that an activity has a direct connection to terrorism, it should immediately provide the

[13] If appropriate, the agency should consult with a JTTF, FIG, or State or major urban area fusion center.

information directly to the responsible FBI JTTF[14] for follow-on action against the identified terrorist activity. In those cases in which the local agency can determine that an activity has a direct connection to a terrorist event or pre-operational planning 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 SLTT agency, fusion center, or Federal agency enters the SAR into an NSI SDR-connected platform. The SAR undergoes a two-part review process by a trained analyst or an investigator to establish or discount a potential nexus to terrorism (i.e., discount that it is reasonably indicative of pre-operational planning associated with terrorism). First, the trained analyst or law enforcement investigator reviews the newly reported SAR information against 16 pre-operational behaviors associated with terrorism that are identified in Part B of this ISE-SAR Functional Standard, keeping in mind—when interpreting the behaviors—the importance of context, facts, and circumstances.[15] The analyst or investigator will then review the input against all available knowledge and information for linkages to other suspicious or criminal activity and determine whether the information reflects Part B behaviors.

Second, if the information reflects one or more Part B behaviors, the officer or analyst will apply his or her professional judgment to determine whether, based on the available context, facts, and circumstances, the information has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). If the officer or analyst cannot make this explicit determination, the report will not be accessible in the NSI SDR, although it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules or reported to the FBI or other law enforcement or homeland security agencies under other legal authorities. However, if that determination is made by the analyst or investigator, the SAR will either be submitted immediately to the NSI SDR or forwarded for secondary review and approval, which may lead to submission to the NSI SDR.

As described in Part B, the activities listed as "Potential Criminal or Non-Criminal Activity" are not inherently criminal behaviors and are potentially constitutionally protected; thus, additional facts or circumstances must be articulated in the incident.

4. Dissemination

Once a SAR has been determined to meet Part B behavior criteria and have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism), the SAR 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. The ISE-SAR is

[14] SARs that do not require an immediate law enforcement response should nonetheless be made available to JTTFs for a coordinated evaluation, including, but not limited to, comparing the information with other holdings available to the FBI as a member of the Intelligence Community.

[15] It is important to note that the analyst or investigator should not make assumptions or presumptions as to why an individual acted or failed to act in a certain way; rather, the determination that the behavior is suspicious should be based on the behavior observed or on documented circumstances.

then uploaded by the submitting agency, where it is immediately provided to the FBI for an assessment-level investigation and made available to all other NSI participants. This allows authorized law enforcement agencies and fusion centers to be cognizant of all terrorism-related suspicious activity in their respective areas of responsibility, consistent with the information flow description in Part C, and allows the FBI to take investigative action as appropriate and in coordination with or with the knowledge of the source agency. Although the ISE-SAR has been shared with all NSI participants, it remains under the ownership and control of the submitting organization (i.e., SLTT law enforcement agency, fusion center, or Federal agency that made the initial determination that the activity constituted an ISE-SAR) and the ISE-SAR is then uploaded to the NSI SDR.

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 SARs without a potential nexus to terrorism have been filtered out. SARs that are vetted, approved, and made available for sharing in the NSI SDR are ISE-SARs and can be presumed by Federal, State, and local analytic personnel to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism), and information derived from them can be used along with other sources to support JTTF or other counterterrorism operations or to develop counterterrorism analytic products. As in any analytic process, however, all information is subject to further review and validation. Analysts must coordinate with the submitting organization for deconfliction and are responsible for obtaining and using any available relevant information in the applicable analytic product. To appropriately safeguard privacy, civil rights, and civil liberties, analytical programs should be conducted in accordance with agency policies and procedures, including privacy policies, and records management schedules and should implement auditing and accountability measures.

Once ISE-SARs are accessible in the NSI SDR, 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.

5. Reevaluation[16]

Operational feedback on the status of ISE-SARs is an essential element of an effective NSI process with important implications for privacy, civil rights, 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. Second, once the FBI assigns and assesses an ISE-SAR, the submitting organization is electronically notified of the FBI field office investigating the SAR and the results of the assessment. These results are maintained in the disposition section of the ISE-SAR for all NSI participants to review.

[16] 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 2008 *NSI CONOPS* for more details.

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 NSI SDR. 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 or the FBI's Guardian Management Unit (GMU) or JTTF acts as a key conduit between the SLTT agencies and other NSI participants. It is important to note that, although many SAR source agencies and ISE-SAR consumers have responsibilities beyond terrorist activities, the NSI ISE-SAR concept is focused exclusively on terrorism-related information. 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 SLTT law enforcement and investigatory personnel and the FBI's JTTFs and/or FIGs.

This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all NSI 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 ISA IPC as appropriate, for both community coordination and consideration. Further, 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.

F. Other Information Sharing Authorities

The ISE-SAR process does not supersede other information or intelligence gathering, collection, or sharing authority, including the authority to share information between and among Federal agencies and SLTT agencies where the information is related to homeland security, terrorism, or other Federal crimes.

Multiple Federal agencies currently have the authority to collect terrorism-related tips and leads. However, only those tips and leads that comply with the ISE-SAR Functional Standard are broadly shared with NSI participants. At the SLTT level, crime and terrorism information, including terrorism-related non-ISE-SAR information, can and should be reported to appropriate Federal agencies based on their relevant legal authorities.[17]

[17] As an example, SLTT agencies may provide terrorism-related source data that leads to the creation of an Intelligence Information Report (IIR), which is ultimately shared with the federal Intelligence Community. In addition, SLTT agencies often enhance existing federal data by providing local context for an assortment of Intelligence Community partners (e.g., Drug Enforcement Administration and DHS components). A third example relates to terrorism-related leads that do not meet the requirements of the *ISE-SAR Functional Standard* but may require investigative follow-up by the FBI. Under the latter circumstance, non-ISE-SAR information may be submitted electronically to the FBI.

It is important to recognize that the multidirectional sharing of non-ISE-SAR information takes place outside the NSI SDR. Consequently, while systems involved in the NSI can be used in the exercise of other agency authorities related to information and intelligence collection, sharing, and analysis, information sharing outside the scope of the *ISE-SAR Functional Standard* must be done in accordance with other agency legal authorities, policies and procedures, and interagency agreements. This means that reports determined not to be ISE-SARs will be handled in accordance with applicable SLTT and other agencies' authorities, policies, and procedures.

G. Protecting Privacy, Civil Rights, and Civil Liberties

Laws that prohibit or otherwise limit the sharing of PII vary considerably between the Federal SLTT levels. The Privacy Act of 1974 (5 USC §552a), as amended, other statutes such as the E-Government Act of 2002, and many governmentwide or departmental regulations establish a framework and criteria for protecting information privacy in the Federal government. The ISE, including NSI participants, must facilitate the sharing of information in a lawful manner, which, by its nature, must recognize, in addition to Federal statutes and regulations, different SLTT, laws, regulations, or policies that affect privacy. One method for protecting privacy, civil rights, and civil liberties while enabling the broadest possible sharing is to anonymize ISE-SAR reports by excluding data elements that contain PII. Accordingly, NSI participating agencies enter ISE-SARs according to their privacy laws and policies and rules governing the sharing of PII, where appropriate.

SECTION III: INFORMATION EXCHANGE DEVELOPMENT DATA MODEL

This ISE-SAR Functional Standard includes a collection of artifacts that support ISE-SAR information exchanges. 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 that 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 agency/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 agency/organization** is the organization that actuates the push of the ISE-SAR to the NSI community. The submitting agency/organization and the source agency/organization may be the same.
>
> The **owning agency/organization** is the organization that owns the target[18] associated with the suspicious activity (see page 21).

[18] The target is a technical term for field of interest that is not readily viewed by someone who queries a particular SAR.

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.
	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.

Privacy Field	Source Class/Element	Source Definition
	Contact Information	
X	Person First Name	Person to contact at the organization.
X	Person Last Name	Person to contact at the organization.
X	E-Mail Address	An e-mail address of a person or organization. [free text field]
X	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 suborganization 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]

Privacy Field	Source Class/Element	Source Definition
	Location	
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]

Privacy Field	Source Class/Element	Source Definition
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).
	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 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]

Privacy Field	Source Class/Element	Source Definition
X	Person Employer ID	Number assigned by an employer for a person such as badge number. [free text field]
	Owning Agency/ 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]
X	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]

Privacy Field	Source Class/Element	Source Definition
	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]
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 nine-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 be used only 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]

Privacy Field	Source Class/Element	Source Definition
	Name Type	Text identifying the type of name for the person. For example, maiden name, professional name, nickname.
	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]

Privacy Field	Source Class/Element	Source Definition
	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 four-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/submitting agency/organization 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.
X	Fusion Center Contact First Name	Identifies the first name of the person to contact at the fusion center. [free text field]
X	Fusion Center Contact Last Name	Identifies the last name of the person to contact at the fusion center. [free text field]
X	Fusion Center Contact E-Mail Address	Identifies the e-mail address of the person to contact at the fusion center. [free text field]

Privacy Field	Source Class/Element	Source Definition
X	Fusion Center Contact Telephone Number	The full phone number of the person at the fusion center who 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 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 to which 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 they can follow up with the submitting 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]

Privacy Field	Source Class/Element	Source Definition
	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 Agency/ 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.
X	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]
X	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]
X	Source Agency Contact E-mail Address	The e-mail address of the person at the agency who is familiar with the record (e.g., law enforcement officer). [free text field]
X	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 URL	The URL to resolve the ISE-SAR information exchange payload namespace.

Privacy Field	Source Class/Element	Source Definition
	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 Agency/ Organization	
	Organization Name	Common Name of the fusion center or NSI participant that submitted the ISE-SAR record to the ISE. [free text field]
	Organization ID	Fusion center or NSI participant's alpha-numeric identifier. [free text field]
	Organization ORI	ORI for the submitting fusion center or NSI participant. [free text field]
	System ID	Identifies the system within the fusion center or NSI 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.

Privacy Field	Source Class/Element	Source Definition
	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 rationale 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.
	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.

Privacy Field	Source Class/Element	Source Definition
	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]

Privacy Field	Source Class/Element	Source Definition
	Vehicle Year	A four-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	VVessel—Official State Registration or Coast Guard Documentation Numbers	An identification issued by either the State or the U.S. Coast Guard. Either number is contained within valid marine documents. State registration numbers should be marked on the forward portion of the hull of the vessel, and documented vessels have a number permanently marked on the vessel's main beam.
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 include the State parks department and the U.S. 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]
X	Vessel MMSI Identification	An identification for the Maritime Mobile Service Identity (MMSI) or a vessel. [free text field]

Privacy Field	Source Class/Element	Source Definition
	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 four-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.
	Vessel Propulsion Text	Text for use when the Boat Propulsion Code does not afford necessary code. [free text field]

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 Between Associated Components	Target Element
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 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 Between Associated Components	Target Element
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)

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/submitting agency/organization 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 suborganization 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 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 flag under which a vessel sails.

SECTION V: INFORMATION EXCHANGE IMPLEMENTATION ARTIFACTS

A. Domain Model

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. Further, 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 readdress business process requirements.

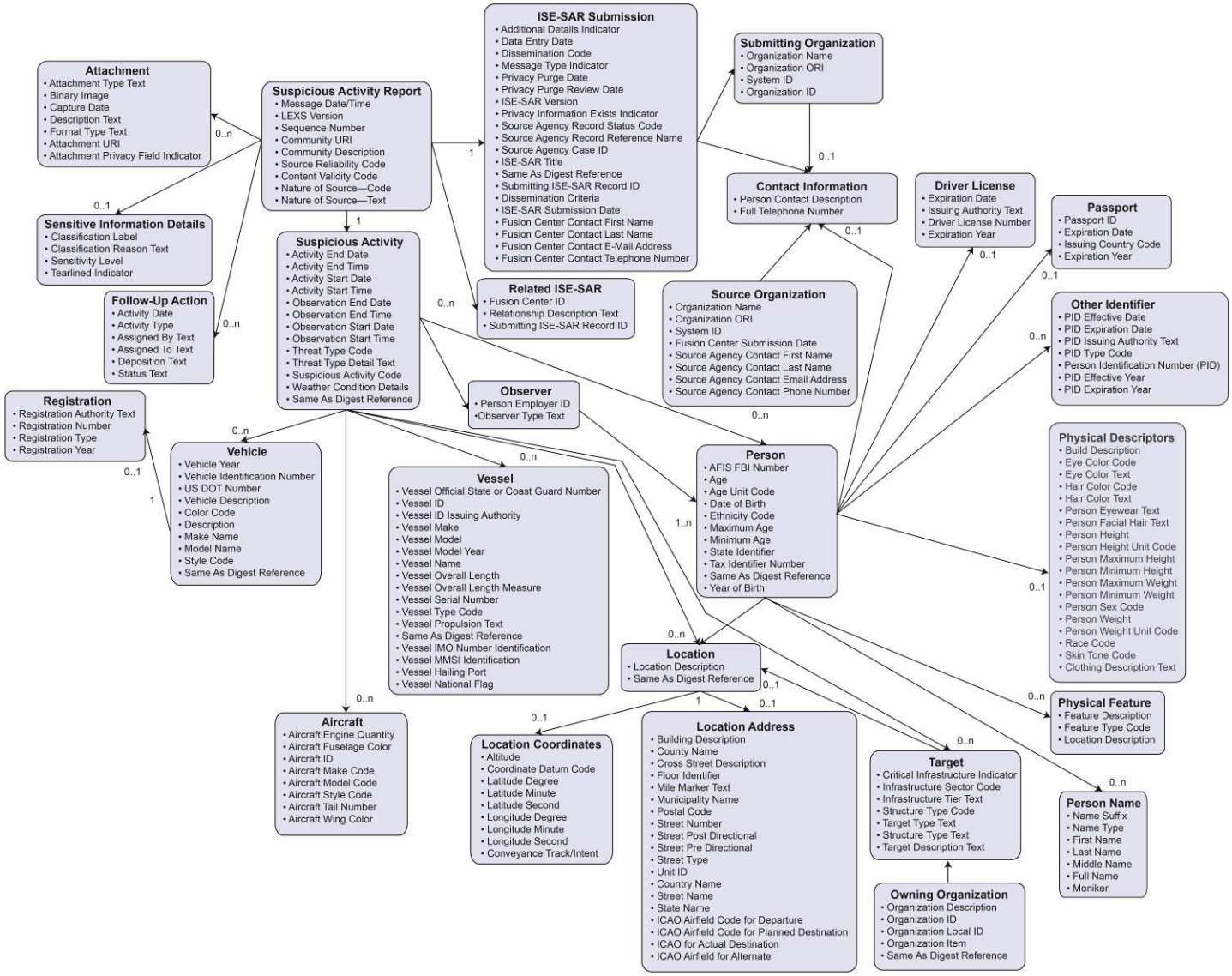

Figure 2 – UML-based Model

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 and 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.

XSL Style Sheet

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

XML Instance

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

PART B—ISE-SAR CRITERIA GUIDANCE

Part B provides a more thorough explanation of ISE-SAR pre-operational behavioral categories and criteria. This guidance highlights the importance of having a trained analyst or investigator take into account the context, facts, and circumstances in reviewing suspicious behaviors to identify those SARs with a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). It is important to understand, however, that the behavioral categories and criteria listed below reflect studies of prior terrorism incidents and are not intended to be limited in any way by the descriptive examples.[19] The descriptive examples outlined below in the third column do not represent all possible examples that relate to ISE-SAR submissions. They are provided as a nonexhaustive list of illustrations of pre-operational behaviors that may support the documentation and submission of an ISE-SAR based on the contextual assessment of the reviewing analyst or investigator.

In order to ensure that Part B is responsive to changes in the threat environment, the ISA IPC will establish a formal process for reviewing and updating the behavioral categories in the first column and the behavioral criteria set forth in the second column. (*See the chart below*.) The process will involve coordination and consultation between and among NSI participants and other stakeholders, who will examine the current body of knowledge regarding terrorism and other criminal activity. This process will result in the issuance of an update to the *ISE-SAR Functional Standard* when revisions are made to either or both of the first or second columns.

As needed, the DHS, in conjunction with the FBI, will guide a *separate* process to allow for interim updates to the descriptive examples contained in the third column of Part B. Updates to the third column will be based on field experience (e.g., emerging threats, trip wire reports, and other intelligence) and will be documented in the change management chart[20] of the *ISE-SAR Functional Standard*, rather than reissuance of the *ISE-SAR Functional Standard* by the PM-ISE.

The nine behaviors identified below as "Potential Criminal or Non-criminal Activity Requiring Additional Information During Vetting" are not inherently criminal behaviors and may include constitutionally protected activities that must not be documented in an ISE-SAR that contains PII unless there are articulable facts or circumstances that clearly support the determination that the behavior observed is not innocent, but rather reasonably indicative of pre-operational planning associated with terrorism. Race, ethnicity, gender, national origin, religion, sexual orientation, or

[19] In addition to the descriptive examples listed in Part B and in order to further enhance NSI participants' understanding of the Part B behavioral categories and criteria, the DHS, in conjunction with the FBI, may develop additional examples to be included in implementation materials (e.g., the *Vetting ISE-SAR Data* guidance) or delivered through training. Additionally, relevant federal and SLTT law enforcement agencies may identify and report additional examples of terrorism behavior within the 16 behavioral categories to the DHS or the FBI.
[20] This chart is included on page 6 of this *Functional Standard*.

gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).[21] The activities listed as "Potential Criminal or Non-Criminal Activity" are not inherently criminal behaviors and are potentially constitutionally protected; thus, additional facts or circumstances must be articulated in the incident. For example, the trained analyst or investigator should document specific additional facts or circumstances indicating that the behavior is suspicious, such as steps to conceal one's location and avoid detection while taking pictures.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY		
Breach/ Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).	• At 1:30 a.m., an individual breached a security perimeter of a hydroelectric dam complex. Security personnel were alerted by an electronic alarm and observed the subject on CCTV, taking photos of himself in front of a "No Trespassing" sign and of other parts of the complex. The subject departed prior to the arrival of security personnel. • A railroad company reported to police officers that video surveillance had captured images of three individuals illegally entering a train station to gain access to a restricted-access tunnel and taking photos of the tunnel.

[21] See footnote 9 for additional guidance.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.	• A state bureau of motor vehicles employee discovered a fraudulent driver's license in the possession of an individual applying to renew the license. A criminal investigator determined that the individual had also fraudulently acquired a passport in the same name and used it to make several extended trips to countries where terrorist training has been documented. • An individual used a stolen uniform from a private security company to gain access to the video monitoring control room of a shopping mall. Once inside the room, the subject was caught trying to identify the locations of surveillance cameras throughout the entire mall.
Theft/Loss/ Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.	• A federal aerospace facility reported a vehicle burglary and the theft of an employee's identification credential, a secure ID token, and an encrypted thumb drive. • An explosives ordnance company reported a burglary of a storage trailer. Items stolen included electric initiators, radios, and other items that could be used in connection with explosives.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Sabotage/ Tampering/ Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.	• A light-rail authority reported the discovery of a track switch that had been wrapped in a length of chain in a possible attempt to derail a passenger train car. • A natural gas company reported the deliberate removal of gas meter plugs on the "customer side" in two separate locations approximately a quarter of a mile apart. One location was a government facility. The discovery was made as the government facility's sensor detected the threat of an explosion.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.	• A federal credit union reported it was taken down for two and a half hours through a cyberattack, and the attacker was self-identified as a member of a terrorist organization. • A state's chief information officer reported the attempted intrusion of the state's computer network by a group that has claimed responsibility for a series of hacks and distributed denial-of-service attacks on government and corporate targets.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.	• A customer-experience feedback agency received a call from a watchlisted individual stating, "Wait till they see what we do to the ATF, IRS, NSA." • A military museum received a threatening letter containing a white powder. The letter claimed a full-scale anthrax attack had been launched in retaliation for crimes committed by the U.S. Armed Forces.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.	• Federal air traffic control personnel reported two separate laser beam cockpit illumination incidents involving different commercial airliners occurring at night and during the take-off phase of flight. The reports revealed that the laser beam in both incidents originated from the same general geographic area, near a major airport on the East Coast. These findings indicate the likelihood of purposeful acts by the same individual. • A chemical facility representative reported an unauthorized helicopter hovering within 50 feet of a chemical tank located in a posted restricted area. An FAA registry search of the tail number was negative, indicating use of an unregistered number, which suggests an attempt to conceal the identity of the plane's owner and/or its place of origin.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL INFORMATION DURING VETTING		
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A tour bus company servicing one of the nation's national monuments reported that a male subject asked a driver many unusual and probing questions about fuel capacity, fueling locations, and fueling frequency such that the driver became very concerned about the intent of the questioning. The male subject was not a passenger. • A guest services employee at a shopping center was questioned by an individual about how much security was on the property. The employee contacted security personnel, who confronted the individual. When questioned by security personnel, the individual quickly changed his questions to renting a wheelchair and then left without being identified. Security personnel reported that the individual seemed very nervous and that his explanations were not credible.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• An individual who refused to identify himself to facility personnel at a shipping port reported that he was representing the governor's office and wanted to access the secure area of a steel manufacturer's space. He was inquiring about the presence of foreign military personnel. The individual fled when he realized that personnel were contacting the security office about his activities. He ran through the lobby and departed in a vehicle with an out-of-state license plate and containing two other individuals. • An individual discharged a fire extinguisher in a stairwell of a hotel and set off the building's fire alarm. This individual was observed entering the hotel approximately two minutes before the alarm sounded, was observed exiting from the stairwell at about the same time as the alarm, and then was observed in the lobby area before leaving the hotel.
Recruiting/ Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A prison inmate reported an effort to radicalize inmates nearing release toward violence. According to the plan, released inmates would go to a particular location for the purpose of obtaining information about attending an overseas terrorist training camp. • An individual reported that a former friend and business associate (a chemist) had recently asked him to participate in a terrorist-cell operation by providing funding to purchase needed equipment. The funding for the operation was reportedly linked to the illegal production of drugs.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.	• A citizen reported to local police that she saw an unknown male crouched down in the back of an SUV with the hatchback open half-way. The subject was videotaping a National Guard readiness center. The vehicle was parked on the side of the road but sped away when the citizen began to approach the vehicle. The citizen could not provide a license tag number. • A citizen observed a female subject taking photographs of a collection of chemical storage containers in the vicinity of the port. The subject was hiding in some bushes while taking photographs of the storage tanks. The citizen reported this information to the city's port police. When the port police officer arrived and approached the subject, she ran to a nearby vehicle and sped off.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Observation/ Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.	• A mall security officer observed a person walking through the mall, filming at waist level, and stopping at least twice to film his complete surroundings, floor to ceiling. The subject became nervous when he detected security personnel observing his behavior. Once detained, the subject explained that he came to the mall to walk around and was simply videotaping the mall for his brother. The camera contained 15 minutes of mall coverage and footage of a public train system, along with zoomed photos of a bus. • Military pilots reported that occupants of multiple vehicles were observing and photographing in the area of residences of the military pilots. The pilots are responsible for the transport of special forces units. The report was made once the pilots realized that they had been individually surveyed by occupants of multiple vehicles during the same time period.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Materials Acquisition/ Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A garden center owner reported an individual in his twenties seeking to purchase 40 pounds of urea and 30 pounds of ammonium sulfate. The owner does not carry these items and became suspicious when the individual said he was purchasing the items for his mother and then abruptly departed the business. • A female reported that a man wanted to borrow her car to purchase fertilizer to add to the 3,000 pounds he had already acquired. When asked why he was acquiring fertilizer, he responded that he was going to "make something go boom." The subject lives in a storage unit and utilizes several other storage units at the location.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A fusion center received information on a watch-listed individual who was making repeated attempts to gain a hazardous materials endorsement for his commercial driver's license even though his immigration status made him ineligible. • A complaint was received from a gun shop about an individual under the age of 21 who had brought multiple groups of students into the gun shop to rent weapons to shoot. They desired to shoot assault rifles and handguns and asked questions about how to get around state and federal laws on weapon possession and transport.

Behavioral Categories	Behavioral Criteria	Select Descriptive Examples
Weapons Collection/ Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A city employee discovered a backpack near a park bench along the route of a planned Martin Luther King Day march in the city. The backpack contained an improvised explosive device. • A suspicious person call resulted in the discovery of three individuals possessing hand-held radios, a military-grade periscope, a 7mm Magnum scoped rifle, an AK-74 assault rifle, a pistol-gripped shotgun, a semi-automatic handgun, a bandolier of shotgun ammunition, dozens of loaded handgun magazines, dozens of AK-74 magazines, Ghillie suits, several homemade explosive devices constructed of pill bottles, blast simulators, and military clothing.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A water company reported that it had security footage of an unknown person breaking into the premises. At 5 a.m., the individual cut through a fence and used a tool to breach a door. Once inside the building, the person took photos of the chlorination system, including the chlorine tank. A pump failure occurred, but it was not certain that this was related to the break-in. • A vehicle containing two individuals was discovered in a secure area of a loading dock at a facility that stores officially designated sensitive chemicals. The vehicle sped off upon discovery by security personnel. Surveillance footage revealed that the individuals gained entry by manually lifting a security gate to the compound.

PART C—ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The information flow begins when a person observes behavior that, based on the circumstances, 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, cyberattacks, 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.[22] Race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion (but attributes may be documented in specific suspect descriptions for identification purposes).[23]	The observer may be a private citizen, a government official, or a law enforcement officer.

[22] A SAR is official documentation of observed behavior that is reasonably indicative of pre-operational planning associated with 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. An ISE-SAR is a SAR (as defined below in 5.t) that has been determined, pursuant to a two-part process, to have a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). ISE-SAR business rules and privacy and civil liberties requirements will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

[23] See footnote 9 for additional guidance.

Step	Activity	Process	Notes
2	Initial Response and Investigation	An official of a Federal, State, local, tribal, or territorial agency with jurisdiction responds to the reported observation.[24] This official gathers additional facts through personal observations, interviews, and other investigative activities. At the discretion of the official, further observation or engaging the subject in conversation may be required. Additional information acquired from such limited investigative activity may then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process, which may include reporting it to the FBI's JTTF. 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 the following: • The Department of Motor Vehicles provides driver's license and vehicle registration information. • The National Crime Information Center provides wants and warrants information; criminal history information; and access to the Terrorist Screening Center, the terrorist watch list, and Regional Information Sharing Systems (RISS). • Other Federal and SLTT 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, citations, incident reports, and arrest reports. The record may be hard and/or soft copy and does not yet constitute an ISE-SAR.

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 an SLTT agency or a field element of a Federal agency. SLTT: Based on specific criteria or the nature of the activity observed, the SLTT law enforcement components forward the information to the State or major urban area fusion center and/or FBI's JTTF for further analysis. Federal: Federal field components collecting suspicious activity forward their reports to the appropriate resident, district, or division office. This information is 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 office, the Federal field component provides 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 SLTT entities or Federal field components.

[24] If a suspicious activity has a direct connection to terrorist activity, the flow moves along an operational path. The information must move immediately into law enforcement operations so as to 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 FBI's JTTF.

Step	Activity	Process	Notes
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 for suspicious behavior based on his or her training and expertise and against ISE-SAR behavior criteria. Second, based on the context, facts, and circumstances, the analyst or investigator determines whether the information meeting the criteria has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism). Once this determination is made, the information becomes an ISE-SAR and is formatted in accordance with the *ISE-SAR Functional Standard*. The ISE-SAR is then shared with the FBI's JTTF and 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 that identify trends and other terrorism-related information and are derived from Federal agencies such as NCTC, DHS, and the FBI. For SLTT 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.
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 made accessible to other law enforcement agencies in the NSI SDR. 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. The ISE-SAR is also made available to the FBI for investigation.	

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 NSI participants and other 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 Joint Counterterrorism Assessment Team (JCAT), formerly 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 SLTT entities and, when appropriate, private-sector entities. JCAT is the mechanism that facilitates the sharing of counterterrorism information with SLTT entities.	

Step	Activity	Process	Notes
8	NCTC Alerts, Warnings, Notifications	NCTC products,[25] informed by the JCAT as appropriate, are shared with all appropriate Federal departments and agencies and with SLTT entities through the State or major urban area fusion centers. The sharing with SLTT entities and the 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 JCAT informed products to help develop geographic-specific risk assessments (GSRAs) to facilitate regional counterterrorism efforts. The GSRAs are shared with SLTT entities and the private sector as appropriate. The recipient of a 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 SLTT entities.
9	Focused Collection	The information has come full circle and the process begins again, informed by another Federal organization's product and the identified information needs of SLTT entities and Federal field components.	

[25] NCTC products 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.

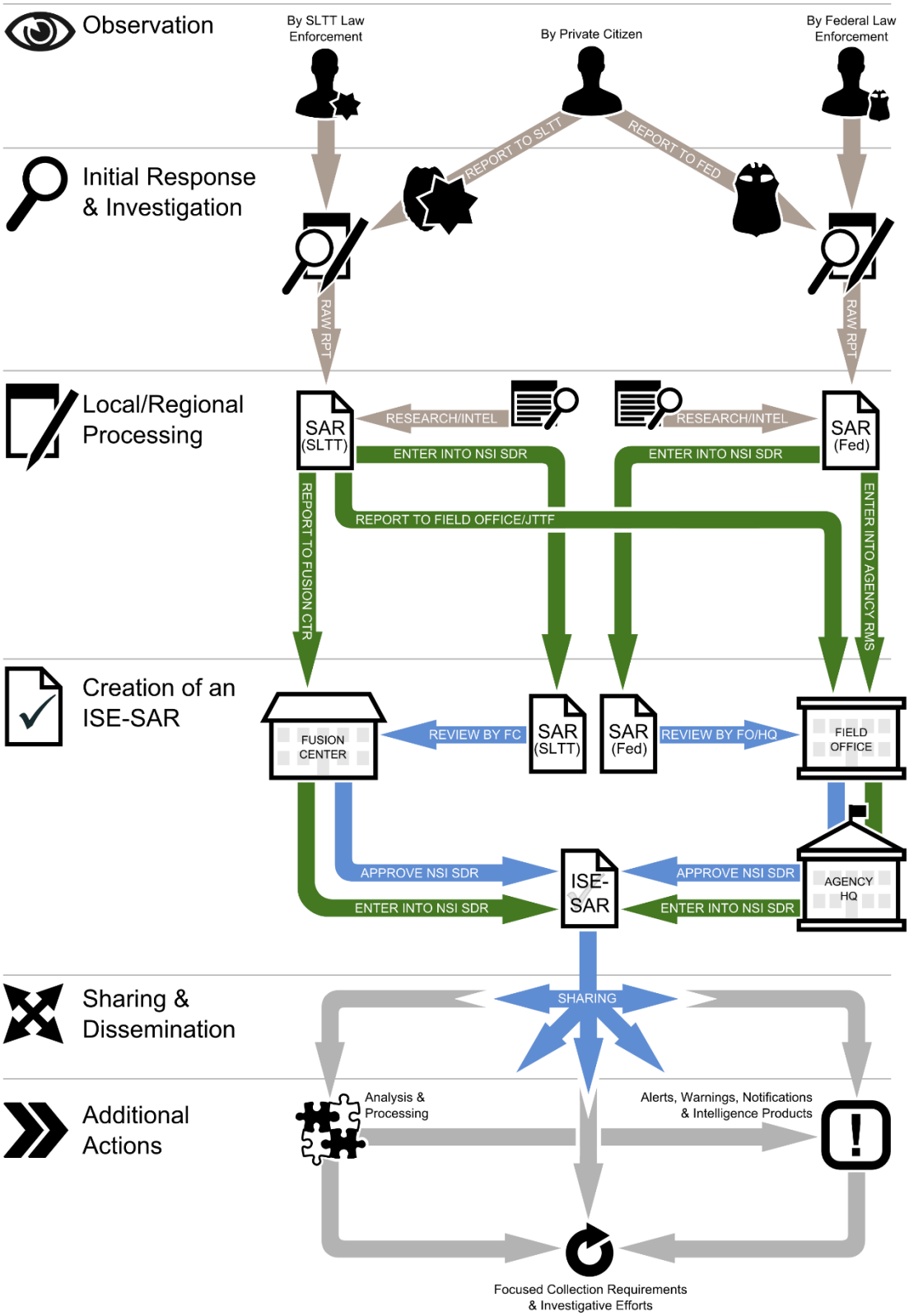
Observation
By SLTT Law Enforcement
By Private Citizen
By Federal Law Enforcement
REPORT TO SLTT
REPORT TO FED
Initial Response & Investigation
RAW RPT
RAW RPT
Local/Regional Processing
SAR (SLTT)
RESEARCH/INTEL
RESEARCH/INTEL
SAR (Fed)
ENTER INTO NSI SDR
ENTER INTO NSI SDR
REPORT TO FIELD OFFICE/JTTF
REPORT TO FUSION CTR
ENTER INTO AGENCY RMS
Creation of an ISE-SAR
FUSION CENTER
REVIEW BY FC
SAR (SLTT)
SAR (Fed)
REVIEW BY FO/HQ
FIELD OFFICE
APPROVE NSI SDR
APPROVE NSI SDR
ISE-SAR
AGENCY HQ
ENTER INTO NSI SDR
ENTER INTO NSI SDR
Sharing & Dissemination
SHARING
Additional Actions
Analysis & Processing
Alerts, Warnings, Notifications & Intelligence Products
Focused Collection Requirements & Investigative Efforts

Figure 3—SAR Information Flow Diagram

PART D—ACRONYMS

CTISS	Common Terrorism Information Sharing Standards
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DOJ	Department of Justice
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
FIGs	Field Intelligence Groups
GRSA	Geographic-Specific Risk Assessment
IEPD	Information Exchange Package Document
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA IPC	Information Sharing and Access Interagency Policy Committee
ISE	Information Sharing Environment
ISE-SAR	Information Sharing Environment-Suspicious Activity Report
JCAT	Joint Counterterrorism Assessment Team
JTTF	Joint Terrorism Task Force
NCTC	National Counterterrorism Center
NIEM	National Information Exchange Model
NSI	Nationwide SAR Initiative
P/CRCL	privacy, civil rights, and civil liberties
P/CL	privacy and civil liberties

PII	personally identifiable information
PM-ISE	Program Manager for the Information Sharing Environment
SAR	Suspicious Activity Report
SDR	Shared Data Repository
SLTT	State, local, tribal, and territorial