TABLE OF CONTENTS

continues to walk his dog, but thinks this behavior is odd. So when he returns to his office, he calls the local sheriff's department to report what he observed.

By the time the deputy arrives the rental truck has departed. Following his training and the department's operational guidelines, the deputy conducts a field investigation, interviews the owner, and gathers as many facts as possible. The owner provides a description of the three men and the license number of the rental truck. Additionally, he provides the deputy with a copy of the storage locker's rental agreement which shows a Washington D.C. address and telephone and a photocopy of the renter's driver's license. The deputy checks the information provided against the "fact based" systems to which he has access and finds that no wants or warrants are outstanding and no additional information is available. Nevertheless, because of related information from the Virginia State Fusion Center regional risk assessment that was included in a recent roll-call training session conducted by the sheriff's office, the deputy does not discount the possibility that this incident may have a connection to terrorism.

The deputy completes his department's field investigation report and turns it in at the end of his shift. The report is subjected to a review following the department's policies and procedures. Based on this review, a decision is made to forward the report to the State Fusion Center for further review. The fusion center analyst reviews the report against criteria for establishing a potential terrorism nexus outlined in the ISE-SAR Functional Standard. The analyst also has access to NCTC reporting and other information that describes the use of remote storage locations to stage equipment and supplies by terrorist organizations in several other countries. Based on her training, experience, and knowledge of terrorist operations, she determines that the event is a suspicious activity with a potential nexus to terrorism.

The fusion center analyst creates an ISE-SAR and stores it in the fusion center's ISE Shared Space. Although, she knows the information is also available to the local Field Intelligence Group (FIG) and JTTF through eGuardian acting as an ISE Shared Space, she decides to walk down the hallway and make sure that the local FBI team is aware of this specific activity. Because this incident appears to be similar to other unusual activity that had come to its attention, the JTTF, in collaboration with local authorities, checks the information and conducts a follow on inquiry. Based on a number of investigative techniques—interviews, fact based data base checks, intelligence reports, surveillance, and others—additional information is acquired, an active case opened, and the ISE-SAR updated to reflect the linkage to an investigation.

In the same timeframe, officers from the Washington Metropolitan Police Department (MPD) are conducting investigative activities related to a tip called into the police concerning a group planning to use an improvised explosive device (IED) in the Washington Capital area. The MPD queries the Virginia and Maryland State Fusion Centers' ISE Shared Spaces for information that might be relevant to their investigative activities concerning the IED tip. Based on the information submitted by the Virginia State Fusion Center, the MPD identifies a vehicle parked near where someone was

seen taking pictures of Federal buildings in Washington, DC and traces the license plate to the same individual who had rented the U-Haul Truck noted earlier in the rural Virginia self-storage facility.

As additional pieces of investigative information are added, officers in all three metropolitan Washington jurisdictions work collaboratively with the JTTF as they move closer to making arrests and disrupting a potential terrorist operation against targets in the national capital area.

Section 4 Steps in the NSI Cycle

This section describes the 12 steps of the NSI cycle shown in Figure 1-1. These steps are grouped into five phases: *Planning, Gathering and Processing, Analysis and Production, Dissemination, and Reevaluation*. Appendix A traces the activities in each step back to the baseline NSIS requirements outlined in Section 2 and also maps them to the 9-step process and information flow in Part C of the ISE-SAR Functional Standard.

Before describing the individual steps, however, it is important to highlight a few points:

- Although presented as a series of discrete steps, the process must be viewed as a continuous cycle that—taken as a whole—constitutes a unified process for using suspicious activity reporting as an important source of CT information.
- The cyclic nature of the process means that the selection of the starting step is somewhat arbitrary. We begin the discussion below with the Planning phase to reinforce the point that an effective ISE-SAR process needs to be driven by threat and risk assessments and conducted by trained personnel.
- The fundamental precept that runs through the entire process is that efforts to detect and prevent terrorist attacks rely on accurate, timely, valid, and reliable information to support law enforcement investigations and other counter-terrorism activities. Accordingly, before any information is posted in an ISE Shared Space as an ISE-SAR it will be subject to multiple levels of review and vetting by trained personnel to ensure that the information is accurate and reliable, has been legally obtained, and has a potential nexus to terrorism.

The NSI cycle as described in this section was developed largely to address the needs and operating methods of Federal, State, and local law enforcement agencies in detecting and preventing terrorist-related criminal activity. Nevertheless, the steps in the NSI cycle are intentionally broad enough to encompass other ISE stakeholders, e.g., private sector organizations or foreign partners, as well. Although many of the steps will allow for inclusion of other sources with little or no change, extending the process to the private sector will likely necessitate variations in the detailed procedures associated with some of the individual steps. Private Sector information may enter the ISE at different points in the SAR cycle. Use of private sector information, moreover, is governed in part by the Protected Critical Infrastructure Information Program, that broadens information sharing between the private sector and the government by providing legal protections of certain sensitive industry information. These differences will be identified and implemented as the NSI evolves and is extended to additional participants.

4.1 Planning

4.1.1 Produce National Threat Assessments

The NSI cycle begins with the production and dissemination of information products about terrorist plans, intentions, and capabilities that are then made available to ISE participants. These threat assessments—typically but not exclusively, produced by Federal agencies—may be derived from multiple information sources, take varying forms, and be issued as classified or unclassified reports. Threat assessments, in turn, help shape the development of local or regional risk assessments by State and major urban area fusion centers.[27]

One important contributor to federally-coordinated threat assessments is the Interagency Threat Assessment and Coordination Group (ITACG) located at the NCTC. The ITACG—staffed by personnel from Federal, State, and local agencies—identifies, reviews, and assesses relevant material of interest to SLT entities. It supports the appropriate dissemination of federally-coordinated terrorism information products through existing websites and distribution channels of DOJ, DHS, and other agencies. Specifically, the ITACG supports the production of three types of reporting:

1. *Alerts, Warnings, and Notifications* and updates of time-sensitive information related to terrorism threats to locations within the United States;
2. *Situational Awareness Reporting* regarding significant events or activities occurring at the international, national, State, or local level to meet the needs of SLT customers; and
3. *Terrorism-Related Strategic and Foundational Assessments* of terrorist threats to the United States that meet the needs of SLT customers.

4.1.2 Conduct Local or Regional Risk Assessments

The threat assessments described in Section 4.1.1 contribute directly to local or regional risk assessments performed by State and major urban area fusion centers in collaboration with local DHS representatives, JTTFs, and FIGs.[28] Whereas threat assessments paint a broad national level picture of terrorist plans, intentions, and capabilities, risk assessments assess the threat in terms of specific local or regional conditions. Accordingly, these regional risk assessments must take into account vulnerabilities and consequences as well as threats. For example, an indication that a terrorist group might be planning attacks on passenger rail transport would be of significant interest to fusion centers in the Northeast corridor of the U.S., but would be

[27] Although these threat assessments are discussed here in the context of the NSI SAR process, they also contribute directly to other ISE processes as well.

[28] In some cases, State Homeland Security Advisors or other officials may have already performed risk assessments. In these cases, the assessments would be modified based on the updated threat information if necessary.

less important to regions not as dependent on commuter railways. Although the responsibility for the risk assessment rests with the fusion center the need to collaborate with other Federal, State, or local agencies as well as private sector organizations in the region is essential. A risk assessment of critical infrastructure, for example, needs to incorporate information that may only be available to DHS or its private sector partners.

4.1.3 Develop Local or Regional Information Requirements

Local or regional risk assessments provide information that should result in more informed and focused gathering of suspicious activity information by adding a more dynamic component to the generic criteria described in Part B of the ISE-SAR Functional Standard. In addition, they form the basis for the fusion center's inputs into the national CT Information Needs process (see Section 4.5.1).

4.1.4 Train Personnel

The *SAR Support and Implementation Project* report highlights the fact that training at all levels is a vital component of an effective process. It calls for, "a training program that reaches all levels of law enforcement personnel so that they can recognize the behaviors and incidents that represent terrorism-related suspicious activity."[29] Although this report understandably dealt primarily with State and local LE agencies, the need for training is equally important for Federal LE personnel participating in the NSI. Specifically, training programs should:

- Ensure that all personnel, regardless of position, understand their roles in the gathering, processing, analysis, and reporting of SAR information;
- See that fusion center personnel understand the overall process and can apply the criteria and related factors for determining that a particular suspicious activity has a potential terrorism nexus;
- Emphasize that SAR reporting is based on observable and clearly defined behaviors and not individual characteristics such as race, culture, religion, or political associations; and
- Include guidance on the protection of privacy and civil liberties.[30]

4.2 Gathering and Processing

4.2.1 Acquire Suspicious Activity Information

Local LE agencies or field elements of Federal agencies gather and document suspicious activity information in support of their responsibilities to investigate potential

[29] Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project, p. 20.
[30] Ibid. p. 21.

criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. Information acquisition begins with an observation of unusual or suspicious behavior that may be indicative of criminal activity associated with terrorism. Such activities include, but are not limited to, surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, possible testing of physical response, or other unusual behavior or sector specific incident.[31]

Regardless of whether the initial observer is a private citizen, a representative of a private sector partner, a government official, or a law enforcement officer, suspicious activity is eventually reported to either a local LE agency or a local, regional, or national office of a Federal agency. The agency responds to the report of information and may gather additional facts through personal observation, interviews and other investigative activities. Context is an important factor in determining whether or not a particular activity is considered suspicious. Taking a photograph of a national monument is more often than not indicative merely of normal tourist behavior. Photographing a nuclear power plant, on the other hand, especially if the persons involved behave surreptitiously, is more likely to cross the threshold into suspicious activity.

When the initial investigation or fact gathering is completed, the investigating official documents the event in accordance with agency policy, local ordinances, and State and Federal laws and regulations. The documentation can be in paper or electronic form, and may be stored in a local information system.

4.2.2 Perform Local Processing

The information is reviewed within a local or Federal agency by appropriately designated officials for linkages to other suspicious or criminal activity in accordance with departmental policy and procedures.[32] Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to the State or major urban area fusion center or JTTF with minimal local processing. Major cities, on the other hand, may have trained CT experts on staff that apply a more rigorous analytic review of the initial reports and filter out those that can be determined not to have a potential terrorism nexus.

[31] Part B of the *ISE-SAR Functional Standard* contains some general criteria for what constitutes terrorism-related suspicious activity. More specific criteria codes are included in the *Findings and Recommendations of the Suspicious Activity Report and Implementation Project*. (Final Draft, June 2008).

[32] If appropriate, the agency may consult with a JTTF, FIG, or fusion center.

4.2.3 Provide SAR to Fusion Center or Federal Agencies

After appropriate local processing, agencies make SARs available to the relevant State or major urban area fusion center.[33] Field components of Federal agencies forward their reports to the appropriate regional, district, or headquarters office employing processes that vary from agency to agency.

Depending on the nature of the activity, the information could cross the threshold of "suspicious" and move immediately into law enforcement operations channels for follow-on action against the identified terrorist activity. In those cases where the local agency can determine that an activity has a direct connection to a possible terrorist-related crime, 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.[34] The FBI uses eGuardian, an unclassified extension of its GUARDIAN system, as the primary mechanism for JTTFs to receive and follow up on investigative leads of terrorism-related crimes. The Bureau is making eGuardian available to Federal, State, local, and tribal law enforcement entities, and has agreed that eGuardian SAR information will be made available to the ISE and *vice versa*. Consequently, eGuardian reports, whether entered directly by the local agency or by the JTTF, will be accessible to the fusion center through ISE Shared Space. Appendix B provides additional information on the roles of ISE Shared Spaces and eGuardian in the NSI.

4.3 Analysis and Production

4.3.1 Process and Analyze SAR at Fusion Center or Federal Agency

The fusion center or Federal agency enters the SAR into its local information system and then performs an additional analytic review to attempt to establish or discount a potential terrorism nexus. First, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria outlined in Part B of the *ISE-SAR Functional Standard*. Second, he or she will review the input against all available knowledge and information for linkages to other suspicious or criminal activity.[35]

[33] N.B., although the ISE deals exclusively with terrorism-related SARs, many fusion centers have an "all crimes" mission. Accordingly, local agencies can forward SARS to the fusion center even though the connection with terrorism may be tenuous or non-existent. The key point is that the SAR will not become an ISE-SAR unless a review at the fusion center establishes a potential terrorism nexus.

[34] The "Attorney General's Guidelines for Domestic FBI Operations," pp. 16-24 identifies three different levels of investigative or information gathering activity—Assessments, Predicated Investigations, and Enterprise Investigations.

[35] Although the *ISE SAR Functional Standard* describes the determination of an ISE-SAR as a two-part process, in many cases the two steps take place almost concurrently.

4.3.2 Determine and Document an ISE-SAR

Based on this review, the officer or analyst will apply his or her professional judgment to determine whether or not the information has a potential nexus to terrorism. If he or she cannot make this explicit determination, the report will not be accessible by the ISE, although it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules. As was already noted in the discussion of processing by local agencies (see Section 4.2.3), where the fusion center or Federal agency can determine that an activity has a direct connection to a possible terrorist-related crime, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation.

4.4 Dissemination

4.4.1 Post ISE-SARs to ISE Shared Spaces

The term "ISE Shared Spaces"—a key element of the ISE Enterprise Architecture Framework (ISE EAF)—is an important implementation approach for developing trust and ISE-wide information sharing. ISE Shared Spaces are networked data and information repositories used to make standardized terrorism-related information, applications, and services accessible to all ISE participants (across the law enforcement, intelligence, homeland security, foreign affairs, and defense communities).[36] The term describes a functional concept, not a specific technical approach. An important consideration is that, although accessible by other authorized ISE individuals and organizations, the Shared Space remains under the management and control of the organization submitting the terrorism-related information—in the particular case of the NSI, ISE-SARs.

Once the determination of a potential terrorism nexus is made, the information becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Functional Standard's IEPD.[37] This ISE-SAR is then stored in the fusion center, JTTF, or other Federal agency's ISE Shared Space where it can be accessed by authorized law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility as well as other ISE participants, including JTTFs through eGuardian. [38] This allows the fusion center to be cognizant of all terrorist-related suspicious activity in its area of responsibility, consistent with the information flow description in the ISE-SAR Functional Standard. Although the information in Shared Spaces is accessible by other ISE participants, it remains under the control of the submitting organization, i.e., the

[36] Information Sharing Environment Enterprise Architecture Framework, Version 2.0 (September 2008), pp. 61-63.
[37] ISE-SAR Functional Standard, Section IV, pp. 12-23.
[38] Version 1 of the *ISE SAR Functional Standard* identifies the organizations that can designate ISE SAR as either (a) State and major urban area fusion centers or headquarters, or (b) field components of Federal Government agencies with a CT mission. One of the options to be evaluated during the EE is whether or not some or all major city police departments should have similar ability.

fusion center or Federal agency that made the initial determination that the activity constituted an ISE-SAR.[39]

4.4.2 Access and Display ISE-SARs

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

Information in ISE Shared Spaces can be searched, accessed, and displayed by authorized ISE investigative and analytic personnel to support their CT missions. Although the ISE is a distributed environment consisting of multiple Shared Spaces at various locations, the intent is the federated search and query approach make it appear to requestors as a single integrated information resource. As a rule, a requestor will first formulate a query that will identify candidate ISE-SARs from all or selected ISE Shared Spaces that satisfy the search criteria. The requestor can then select and display individual reports of interest.

During the EE, requestors can display ISE-SARs, but will not be authorized to download or otherwise manipulate them. The intent for the NSI, long-term, however is that analysts would be able to retrieve, display, and download ISE-SARs and integrate them into local or shared applications such as geospatial display or manipulation software.

Depending on privacy policy and procedures established for the NSI as a whole or by agencies responsible for individual Shared Spaces, requestors may only be able to view reports in the Summary Format of the ISE-SAR IEPD, i.e., without privacy fields. In these cases, requestors may contact the submitting organization directly to discuss the particular report more fully and obtain access to the information in the privacy fields if appropriate.

Once ISE-SARs are accessible, they can be used to support a range of CT analytic and operational activities. So this step involves the actions necessary to integrate the use of SAR information into existing CT analytic and operational processes including efforts to "connect the dots," identify information gaps, and develop formal analytic products. As a

[39] Section IV of the ISE-SAR Functional Standard differentiates between the "Source Organization" (the agency that initiates the report) and Submitting Organization" (the agency that provides the ISE-SAR to the ISE), noting that, in some cases, they can be the same. See *ISE-SAR Functional Standard*, p. 12.

result, there needs to be a tight linkage between the activities in this step and those of the Reevaluation and Threat Assessment steps described in Sections 4.5 and 4.1.1 respectively

4.5 Reevaluation

4.5.1 Establish a National Framework for CT Information Needs

In response to the NSIS requirement to facilitate "the exchange of coordinated sets of requirements and information needs across the Federal and non-Federal domains," the NCTC, FBI, DHS, and the PM-ISE are establishing a framework to enable sharing CT information needs among Federal agencies and SLT organizations.[40] When fully implemented, this process will incorporate a mechanism for SLT agencies to input terrorism information needs and provide for annual review, revision, and sharing of CT information needs across all levels of government.

4.6 Feedback

Feedback is not a single discrete step; it takes place continuously throughout the NSI cycle. But continuous feedback is an essential part of the NSI process with important implications for privacy and civil liberties. It encompasses both operational feedback to ISE participants—information regarding the status of ISE-SARs—and administrative feedback—information regarding possible future process improvements, e.g., best practices, or changes to the ISE-SAR Functional Standard. Administrative feedback is provided through the NSI governance process described more fully in Section 6.

Operational feedback on the status of ISE-SARs is an essential element of an effective NSI process. 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 agencies know that their initial suspicions have some validity. Moreover, the process must support notification of all ISE participants when further evidence determines that an ISE-SAR was designated incorrectly so that the original information does not continue to be used as the basis for analysis or action. This type of feedback can support agency redress processes and procedures where appropriate. To foster collaboration among participants and ensure accountability, at least initially, operational feedback mechanisms should be under human control, employing simple techniques such as telephone or electronic mail.

[40] NSIS, p. 11.

Section 5 The ISE-SAR Evaluation Environment

5.1 Objectives

ISE Evaluation Environments represent a low risk approach for testing and evaluating ISE policies, business processes, capabilities, architectures, and standards by sponsoring efforts that implement and evaluate solutions to operational needs in a relatively controlled environment.[41] An EE is not merely a proof-of-concept or technology demonstration, but serves as a preliminary phase of a longer term effort that assesses and refines processes and capabilities prior to full-scale operational use.

The ISE-SAR Evaluation Environment serves as a microcosm of the broader NSI—a smaller-scale implementation testbed. It provides a platform to test and evaluate the steps in the NSI cycle described in Section 4 in a real world setting. It allows modifications and improvements to be made in a controlled way with the goal of publishing a guide or template for Federal and SLT agencies to use in establishing a national process for gathering, documenting, processing, analyzing and sharing of terrorism-related suspicious. Specific objectives include:

1. Improving operational processes at local LE agencies and Fusion Centers by providing capabilities to document, store, and share terrorism-related SARs;
2. Testing and validating fundamental ISE EAF concepts and core services;
3. Incorporating “Lessons-Learned” and “Best Practices” into an implementation guide and template for establishment of a national ISE-SAR process;
4. Informing ISE Investment Planning; and
5. Issuing an updated version of the ISE-SAR Functional Standard.

5.2 Participating Organizations

The ISE-SAR EE is sponsored and funded by the PM-ISE who is responsible for overall direction and oversight. DOJ/BJA provides planning, project management, and implementation services. The Office of the Assistant Secretary of Defense for Homeland Defense and America’s Security Affairs (ASD HD&ASA) participates in support of the DoD force protection/anti-terrorism mission. DHS representatives assigned to fusion center will support ISE-SAR activities at participating sites, and at least one DHS component organization will implement an ISE Shared Space accessible by other EE participants. The FBI will participate in the EE primarily through its JTTFs, some of which are collocated with fusion centers, who will use the eGuardian system both as a source of CT investigative leads as well as a vehicle for accessing ISE Shared Spaces.

[41] ISE Implementation Plan (November 2006), p. 30.

In addition to the Federal organizations, the MCCA, the CICC, the International Association of Chiefs of Police (IACP), and the Major County Sheriffs' Association (MCSA) will help provide oversight from the State and local perspective.

ISE Shared Spaces are currently being installed at three State fusion centers—New York, Florida, and Virginia. The latter two will also serve as testbeds for cross sharing between the LE and Defense (force protection/anti-terrorism) communities. In addition, up to nine sites, including a mix of State and major urban areas fusion centers as well as DHS and FBI (eGuardian), will be added over the next year, providing a user base of sufficient size and diversity to test the viability and scalability of the process. Access to the EE will be available through multiple Sensitive but Unclassified (SBU) networks or portals—Law Enforcement Online (LEO), the Regional Information Sharing System (RISS), and the Intelligence segment of the Homeland Security Information Network (HSIN). The entry point for federated searches and retrievals of ISE Shared Spaces is BJA's National Criminal Intelligence Resource Center (NCIRC).Figure 5-1 shows a top level view of the ISE-SAR EE.

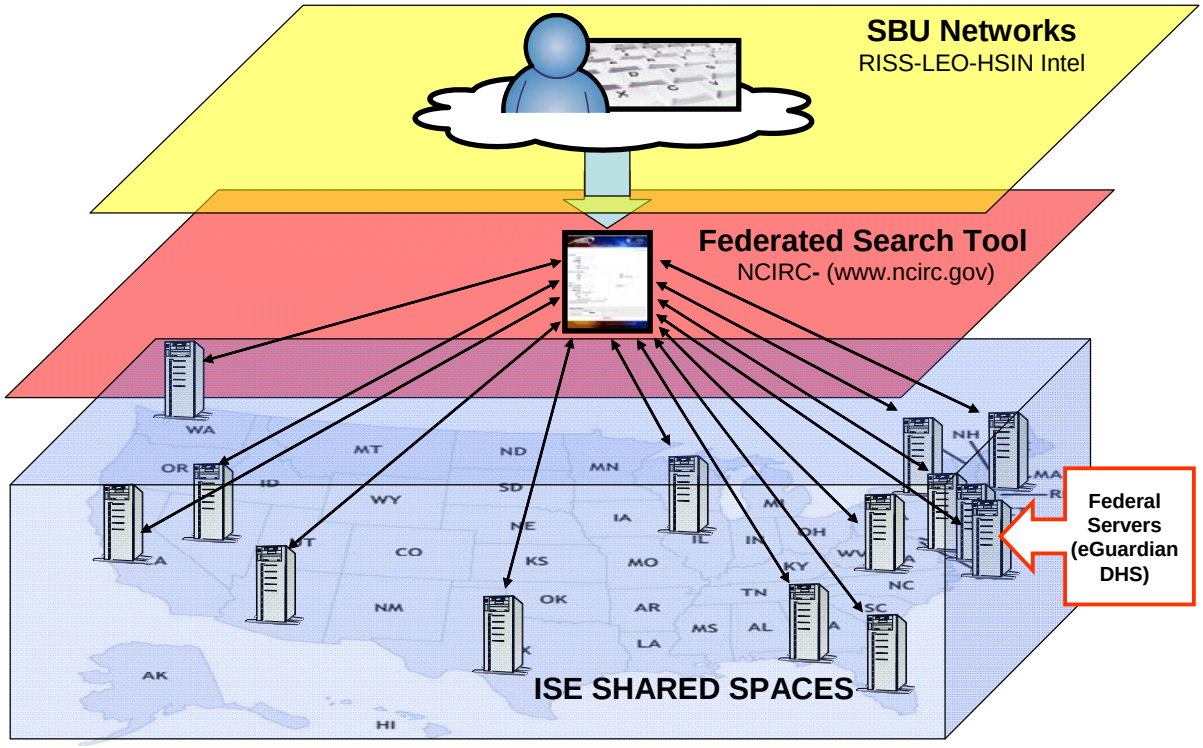

Figure 5-1. Top-level View of ISE-SAR Evaluation Environment

4. ***DOJ/FBI***, as the lead Federal organization responsible for investigating terrorism-related crimes,
   a. Assists NCTC in establishing and managing a process that incorporates the CT information needs of SLT organizations;
   b. Develops intelligence products—including products based in whole or in part on analysis of ISE-SARs where appropriate—and makes them available to Federal and SLT customers;
   c. Shares FBI terrorism-related suspicious activity information with sites participating in the ISE-SAR EE;
   d. Trains personnel on their roles and responsibilities in the NSI process as appropriate;
   e. Assists in the planning and execution of the EE and collaborates with sites to develop local or regional risk assessments and information requirements; and
   f. Serves as a member of the ISE-SAR Steering Committee.
5. ***DoD/ASD (HD&ASA)***
   a. Provides broad direction, coordination, and oversight of SAR activities for all DoD components;
   b. Establishes one or more DoD sites as part of the ISE-SAR EE;
   c. Ensures that information about suspicious activity relating to the protection of DoD personnel and facilities is shared with sites participating in the EE;
   c. Trains DoD personnel on their roles and responsibilities in the NSI process as appropriate;
   d. Shares DoD EE evaluation criteria, feedback, and evaluation reports reciprocally with EE partners; and
   e. Serves as a member of the ISE-SAR Steering Committee.
6. ***DHS/Office of Operations Coordination and Planning***
   a. Assists in coordinating SAR activities for DHS Components utilizing the DHS information sharing governance structure where appropriate;
   b. Supports State and major urban area fusion center SAR analytic activities in coordination with the DHS State and Local Program Management Office;
   c. Assists NCTC in establishing and managing a process that incorporates the CT information needs of SLT organizations;
   d. Develops intelligence products—including products based in whole or in part on analysis of ISE-SARs where appropriate—and makes them available to Federal and SLT customers;
   e. Participates in the ISE-SAR EE through one or more of its component organizations;

f. Ensures that information with a potential nexus to terrorism as outlined in the ISE-SAR Functional Standard is shared with State and major urban area fusion centers participating in the EE;

g. Trains DHS personnel on their roles and responsibilities in the NSI process as appropriate;

h. Through DHS fusion center analysts, assists in the planning and execution of the EE and helps sites develop local or regional risk assessments and information requirements; and

i. Serves as a member of the ISE-SAR Steering Committee.

7. ***NCTC***

a. Working with the Office of the DNI (ODNI), DHS, and the FBI, establishes and manages a process that consolidates and shares CT information needs among Federal agencies and SLT organizations;

b. The ITACG, a component of the NCTC, informs and helps shape national intelligence community products—including products based in whole or in part on analysis of ISE-SARs where appropriate—by providing advice, counsel and subject matter expertise to better meet the needs of SLT organizations, and facilitates dissemination of these products to SLT agencies through established channels; and

c. Serves as a member of the ISE-SAR Steering Committee.

8. ***ODNI/Policy Plans and Requirements/Homeland Security and Law Enforcement***

a. Supports NCTC in establishing and managing the CT Information Needs process;

b. Leads the effort to establish a framework for how ISE-SARs will be used as part of the CT analysis process; and

c. Serves as a member of the ISE-SAR Steering Committee.

9. ***Other ISC member agencies***

a. Ensure that agency processes that support gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity are conducted in accordance with the ISE-SAR Functional Standard and this CONOPS;

b. See that adequate resources are programmed and budgeted to support agency participation in the NSI; and

c. Train personnel on their roles and responsibilities in the NSI process as appropriate.

evaluating the EE and the broader NSI, the PM-ISE and ISE-SSC will adopt strategic and performance goals for the NSI along with specific performance targets and measures that help assess NSI progress and performance.

Reference	NSIS Requirement	NSI Cycle[47]	ISE-FS-200 Ver. 1[48]
2.2.3.2.	Using this assessment to identify priority information *needs*	Section 4.1.3	N/A
2.2.3.3.	Identification of data sources and repositories of prioritized information	Sections 4.1.2 - 4.1.3	N/A
2.2.3.4.	Maintaining an information gathering and reporting strategy utilizing existing local capabilities	Sections 4.1.3 - 4.1.4	N/A
2.2.3.5.	Developing, implementing, and maintaining a method for communicating information priorities to local gatherers of information	Sections 4.1.3 - 4.1.4	N/A
2.2.3.6.	Ensuring that priority information, including SARs, are disseminated to and evaluated by appropriate government authorities and appropriate critical infrastructure owners and operators	Sections 4.4.1 - 4.4.2	Steps 1-6
2.2.3.7.	Ensuring that priority information, including SARs, is reported to national entities to support its inclusion into national patterns and trends analysis and other States and localities to support regional trends analysis	Sections 4.4.1 - 4.4.2	Steps 1-7
2.2.3.8.	Identifying system requirements that support a unified process for reporting, tracking, and accessing SARs	Sections 4.1.1 - 4.5.1	N/A
2.2.3.9.	Defining a feedback mechanism	Section 4.5.2	N/A

Appendix B – The NSI as an Integrated ISE Shared Space Environment

Overview

The goal of the NSI is that Federal, State, local, tribal, and law enforcement organization across the United States participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity. The NSI is an umbrella initiative encompassing multiple, but complementary, efforts each of which plays an important role in supporting efforts by Federal, State, local, and tribal agencies to detect and prevent terrorist crimes and to bring offenders to justice. The emphasis is on improving and standardizing policies, processes, and procedures for sharing SARs with a potential terrorism nexus rather than employing specific automated tools or techniques.

Two important components of the unified NSI process are:

- An ISE initiative that promotes the sharing of terrorist-related SARs among authorized users at local law enforcement agencies, State and major urban area fusion centers, and federal agencies such as DHS through use of distributed ISE Shared Spaces (dedicated servers located at fusion centers); and
- The FBI's eGuardian system that uses a centralized database and associated tools to support JTTFs in assessing and investigating terrorism-related crimes and also to improve sharing of terrorism information between JTTFs and local agencies. The DoD has also decided to use eGuardian as its repository of ISE-SARs gathered as part of the ISE-SAR EE in support of its force protection/anti-terrorism mission.

Although the two efforts have some similarities—both enable improved sharing of terrorism-related SARs; both implement the IEPD from the ISE-SAR Functional Standard; and both incorporate provisions that help protect privacy and civil liberties—they form two distinct but complementary parts of a single unified nationwide initiative. This appendix clarifies the roles of eGuardian and ISE Shared Spaces and establishes fundamental principles for their operational use and interaction during the ISE-SAR EE.

For a number of years the FBI has relied on the Guardian system, operating at the Secret level, as its principal tool for managing assessment and investigation of terrorism-related crimes. Although access to classified information by State and local agencies has expanded over the last few years, it is still far from universal. Consequently, the information in Guardian is still inaccessible to many Federal, State, and local law enforcement agencies.

Development of eGuardian, a system that operates in the SBU domain, as an adjunct to Guardian reflected the realities that initial indications of such crimes were generally not classified and that JTTF operations would be improved if there were broader sharing of information and greater collaboration with local law enforcement agencies. The FBI envisions eGuardian as the primary mechanism JTTFs will use to follow up on investigative leads of potential terrorism-related crimes, using Guardian more as a system for managing active terrorism cases. The Bureau is making eGuardian available to Federal, State, local, and tribal law enforcement agencies, and has agreed that eGuardian terrorism-related SAR and threat assessment information will be made available to all participants in the ISE-SAR EE. Consequently, eGuardian reports—whether entered by a local agency, fusion center, or JTTF—will be accessible either directly through eGuardian or through federated searches and queries of SARs stored in ISE Shared Spaces.

The concept of ISE Shared Spaces—responding directly to the Congressional requirement that the ISE provide "a decentralized, distributed, and coordinated environment", for sharing of terrorism related information[49]—is a fundamental element of the ISE Enterprise Architecture Framework. ISE Shared Spaces are simply mechanisms that make standardized terrorism-related information accessible to authorized ISE users. Although accessible by other ISE participants, the information in an ISE Shared Space—in the case of the NSI, ISE-SARs—remains under the management and control of the organization originally that originally submitted the terrorism-related information to the ISE, i.e., the fusion center or Federal agency that determined that the activity met the criteria for designation as an ISE-SAR.

Information from ISE Shared Spaces is made available to eGuardian in two ways. First, since one of eGuardian's functions is to serve as an ISE Shared Space, all ISE-SARs will be accessible to users as soon as they are entered in any ISE Shared Space. Second, in those cases where it can determine that a reported activity has a clear connection to a possible terrorist-related crime, the local agency or fusion center will—in addition to posting the report in its Shared Space—provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation.

The ISE-SAR EE serves as a microcosm of the broader NSI—a smaller-scale implementation testbed with participation by Federal agencies (DoD, DOJ, and DHS) as well as State and major urban area fusion centers. It provides a platform to test and evaluate the steps in the NSI cycle, allowing modifications and improvements to be made in a controlled manner to form the basis for an improved process to be used nationwide. The remainder of this appendix outlines fundamental principles that will govern the way that ISE Shared Spaces and eGuardian will operate during the ISE-SAR EE.

[49] Intelligence reform and Terrorism Prevention Act of 2004, P.L. No. 108-458 (December 2004), §1016(b)(2).

Guiding Principles

1. *Collaboration.* Detecting and preventing terrorism-related crimes requires close working collaboration among law enforcement agencies at all levels of government. Although the FBI leads the effort through its more than 100 JTTFs, State and local agencies provide unique knowledge and capabilities that are essential to the overall effort. Collaborative efforts that allow each agency to contribute its specialized local knowledge and insights to the overall effort will significantly improve the chances of detecting and preventing attacks on our people and institutions.
2. *Transparency.* A principle objective of the NSI is full and transparent exchange of terrorism-related SARs among all Federal, State, and local participants in the EE regardless of which system is used to initially enter the information. In addition to supporting JTTFs in assessments and investigations, eGuardian will function as another ISE Shared Space so that federated queries by law enforcement officers/agents or analysts will return eGuardian results along with results from the ISE Shared Spaces at State or major urban area fusion centers. Conversely, eGuardian users will be able to access ISE-SAR information from participating fusion centers as well as from eGuardian's database. In addition, the FBI plans to download relevant unclassified entries that were initially placed in Guardian to eGuardian where they will be available to all participants with SBU access.
3. *Local Control.* Although information will be shared as broadly as possible, the process relies on a distributed system of sharing that maintains local control over ISE-SAR information. The determination to provide an ISE-SAR immediately to the responsible JTTF through eGuardian for use as the basis for an assessment or investigation of a terrorism-related crime is made by the responsible local agency or fusion center. SARs stored in ISE Shared Spaces, even those directed to a JTTF as investigative leads, remain in the submitting organization's ISE Shared Space. They are still under the control of the agency that made the determination that the activity had a potential nexus to terrorism and can only be modified or deleted by that organization.[50]
4. *Local Process Variations.* Related to the principle of local control is the recognition that, although all participants will follow the general NSI process, the details of that process will vary from one locality to another. The degree of collaboration between State or major urban area fusion centers and JTTFs will not be the same in all areas of the country. Nor will the processes used by a small town or county be the same as those that work for a major urban area. The ISE strives to rationalize, standardize, and harmonize processes and policies wherever possible, but recognizes they must be tailored to local conditions. Consequently, the ISE promotes what are referred to as "mostly common," rather

[50] The ISE-SAR Functional Standard refers to the agency that originates the SAR as the *source organization* and the organization that provides the information to the ISE as the *submitting organization*. In some cases the source and submitting organizations may be the same.

than identical, capabilities and processes.[51] The EE will identify "best practices" from all participants that will help to better standardize and harmonize SAR processes across the ISE, but some local variations will always remain.

5. *Feedback and Notification.* Clear and effective feedback is an integral part of the NSI process. Feedback takes place continuously throughout the process; it is not a single discrete step. Examples include:
   a. Submitting organizations notify source agencies when information they provide is designated as an ISE-SAR;
   b. All EE participants are notified when further evidence determines that an ISE-SAR was designated incorrectly so that the original information does not continue to be used as the basis for analysis or action;
   c. Local agencies or fusion centers notify the JTTF of potential investigative leads when they submit a record to eGuardian; and
6. *Confidence Indicators.* Although the details need to be worked out, a standard mechanism for grouping SARs into a few categories according to the likelihood that they truly reflect precursor activities of a terrorist attack will be adopted and implemented. This categorization will assist in improving the SAR process by incorporating established patterns of suspicious activity that prove to be more reliable indicators of potential terrorist behavior and by better enabling agencies to apply limited analytic resources to highest priority events.
7. *Data Entry Minimization.* The EE will minimize unnecessary data entry wherever possible. In particular, no additional data entry will be required when a fusion center determines that a report meets the criteria for an ISE-SAR and will be posted to an ISE Shared Space or when a local agency or fusion center decides to forward an existing ISE-SAR to eGuardian for JTTF assessment or investigation.

[51] Annual Report to the Congress on the Information Sharing Environment (June 2008), p. 3.

Appendix C – Acronyms and Abbreviations

ASD	Assistant Secretary of Defense
BJA	Bureau of Justice Assistance
CICC	Criminal Intelligence Coordinating Council
CONOPS	Concept of Operations
CSG	Counterterrorism Security Group
CT	Counterterrorism
CTISS	Common Terrorism Information Sharing Standards
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
EE	Evaluation Environment
FBI	Federal Bureau of Investigation
FIG	Field Intelligence Group
FS	Functional Standard
Global	Global Justice Information Sharing Initiative
HD&ASA	Homeland Defense and America's Security Affairs
HSIN	Homeland Security Information Network
IACP	International Association of Chiefs of Police
IED	Improvised Explosive Device
IEPD	Information Exchange Package Document
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISC	Information Sharing Council
ISE	Information Sharing Environment
ISE EAF	Information Sharing Environment Enterprise Architecture Framework
ISE-SAR	Suspicious Activity report determined to have a potential nexus to terrorism
ISE-SSC	ISE-SAR Steering Committee
ITACG	Interagency Threat Assessment and Coordination Group
JTTF	Joint Terrorism Task Force
LAPD	Los Angeles Police Department
LE	Law Enforcement
LEO	Law Enforcement Online

MCCA	Major Cities Chiefs Association
MCSA	Major County Sheriffs' Association
MPD	[Washington, DC] Metropolitan Police Department
NCIRC	National Criminal Intelligence Resource Center
NCTC	National Counterterrorism Center
NIEM	National Information Exchange Model
NSI	Nationwide SAR Initiative
NSIS	National Strategy for Information Sharing
ODNI	Office of the Director of National Intelligence
OJP	Office of Justice Programs
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
RISS	Regional Information Sharing System
SAR	Suspicious Activity Reporting
SBU	Sensitive but Unclassified
SLT	State, local, and tribal