NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

CONCEPT OF OPERATIONS

Prepared by the
Program Manager, Information Sharing Environment

Version 1, December 2008

NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

CONCEPT OF OPERATIONS

Prepared by the
Program Manager, Information Sharing Environment

Version 1, December 2008

TABLE OF CONTENTS

Section 1 Introduction

1.1 Background

The Nationwide Suspicious Activity Report (SAR) Initiative as described in this Concept of Operations (CONOPS) builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime—and establishes a process whereby SAR information can be shared to help detect and prevent terrorism-related criminal activity.[1] Although not specifically using the term "suspicious activity reporting," the 9/11 Commission Report is replete with examples of opportunities lost because available information was inaccessible outside a specific agency or narrow community of interest because of what the Commission referred to as "the human or systemic resistance to sharing information." The Commission recognized that Federal, State, local, and tribal (SLT) governments have access to information which could, when synthesized with information from other sources, help identify precursor activities of terrorist attacks.[2] The challenge is to make this information available to those who need it in time to protect our people and institutions while at the same time ensuring that information privacy, civil liberties, and other legal rights are adequately protected.

In the fall of 2005, recognizing that suspicious activity reporting could make an important contribution to the Nation's efforts to combat terrorism, the Counterterrorism Security Group (CSG), an arm of the National Security Council, tasked the National Counterterrorism Center (NCTC) to work with the counterterrorism (CT) community to develop options for improving the value of SAR to the CT mission. In September 2006, the CSG directed the Program Manager for the Information Sharing Environment (PM-ISE) to build on this work and incorporate it into implementation planning activities for the Information Sharing Environment.

Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directs the President to establish the ISE—defined broadly as an approach that facilitates the sharing of terrorism information—"in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[3] The purpose of the ISE is to rationalize, standardize, and harmonize the policies, business processes, standards, and systems used to share terrorism-related information. Although the intent is to achieve as much uniformity as possible across the ISE, actual

[1] This CONOPS uses the term "Suspicious Activity Report" in its most general sense; see Section 2.1 for a formal definition. Accordingly, this term or its abbreviation (SAR) should not be confused with the very specific use of the same term in the Bank Secrecy Act of 1970, 31 USC 5311-5330, (as amended), and 31 CFR §103.18 where it describes a standardized report that banks are required to make on suspicious banking transactions relevant to a possible violation of law or regulation.

[2] Final Report of the National Commission on Terrorist Attacks Upon the United States (July 2004), pp. 416-419.

[3] *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law No. 108-458 (December 2004), §1016(b)(1). The responsibilities of the Program Manager are spelled out in §1016(f)(2).

implementations will vary depending on different mission needs and available capabilities. Accordingly, the ISE goal is to achieve "mostly common" capabilities tailored to the needs of each participant. The Program Manager plans for and oversees the implementation of the ISE in consultation with an interagency Information Sharing Council (ISC). Additional information on the ISE can be found on the Program Manager's website at http://www.ise.gov/.

The CSG-directed effort resulted in adoption of a common definition for SAR, agreement on a common set of SAR data elements, and development of a preliminary set of criteria to assist in determining whether a report of suspicious activity should be designated as an ISE-SAR, i.e., one with a potential terrorism nexus.[4] Further impetus for an integrated nationwide process for sharing terrorism-related SARs across the ISE came from the recommendations responding to Presidential Guideline 2, approved by the President in November 2006, that called for the development of "processes and protocols for ensuring that priority information [to include SARs] are reported to the appropriate law enforcement (LE) authorities and national entities to support inclusion into national patterns and trends analysis."[5]

In October 2007, the President issued the *National Strategy for Information Sharing* (NSIS). The NSIS built on the foundational work already done under the ISE Implementation Plan to outline an explicit set of requirements (described in more detail in Section 2) for a unified SAR process. The publication of the NSIS helped give rise to a number of related activities, each of which addressed different aspects of such a unified SAR process. These included:

- The PM-ISE, through the Common Terrorism Information Sharing Standards (CTISS) Committee of the ISC, issued an ISE functional standard that described an ISE-SAR business process, information flow, and an Information Exchange Package Document (IEPD)—part of the National Information Exchange Model (NIEM) standards program—to better enable ISE participants to share ISE-SAR information in a standard format.
- The Departments of Justice (DOJ) and Defense (DoD) launched a PM-ISE-sponsored evaluation environment (EE) aimed at testing and evaluating the IEPD and business process components of the ISE-SAR Functional Standard.
- The Los Angeles Police Department (LAPD) established a department-wide process for gathering, processing, and sharing terrorism-related SARs. This process, which is consistent with the ISE-SAR Functional Standard, uses e-learning and roll call training to inform officers how to recognize potential

[4] The terms "SAR" and "ISE-SAR" are defined formally on page 1 of the *Information Sharing Environment (ISE) Functional Standard, Suspicious Activity Reporting (SAR), ISE-FS-200* (January 2008). The functional standard, along with information about the CTISS program, is available on the PM-ISE website, http://www.ise.gov/pages/documents.html.

[5] Guideline 2 – Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector (November 2006), p. 18. The report is available at http://www.ise.gov/docs/guidance/guideline%202%20-%20common%20sharing%20framework.pdf.

terrorist activities while providing standardized reporting codes that facilitate the reporting and review of terrorism-related suspicious incidents.

- Building on the LAPD experience, the DOJ Bureau of Justice Assistance (BJA) an element of the Office of Justice Programs (OJP), the Major Cities Chiefs Association (MCCA); the Criminal Intelligence Coordinating Council (CICC), a part of DOJ's Global Justice Information Sharing Initiative (Global); and the Department of Homeland Security (DHS) sponsored a SAR Support and Implementation Project study that made a number of important recommendations that were adopted by the MCCA leadership in June 2008 and endorsed by the CICC in September.[6]
- The Federal Bureau of Investigation (FBI) began operational tests of a new system called eGuardian that supports Joint Terrorism Task Force (JTTF) investigations of terrorism-related crimes. eGuardian is an unclassified extension of an earlier classified system called Guardian that provides access to a much broader population including State, local, and tribal law enforcement agencies. The intent is that all suspicious activity reporting information in eGuardian will be accessible to the ISE and vice versa.
- The PM-ISE established an ISE-SAR Steering Committee, comprised of the major Federal, State, and local stakeholders, to provide strategic direction and serve as a forum for articulating and addressing ISE-SAR process requirements.

1.2 The Nationwide SAR Initiative

The Nationwide SAR Initiative (NSI) is an outgrowth of these and other activities—responding directly to the mandate to establish a "unified process for reporting, tracking, and accessing [SARs]" as called for in the National Strategy.[7] That end-to-end process is depicted in Figure 1-1 as a cycle of 12 discrete steps (described in detail in Section 4) that includes all activities required to address the NSIS requirement.[8] The long term goal is that most Federal, State, local, tribal, and law enforcement organizations will participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially terrorism-related. In addition to government agencies, private sector organizations responsible for critical Infrastructure and foreign partners are also potential sources for terrorism-related SARs.

The NSI is not a single monolithic program, but is rather a coordinated effort that leverages and integrates all ISE-SAR-related activities into a national unified process. Its strategy is to develop, evaluate, and implement common processes, and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-

[6] Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project, Final Draft (August 2008). The report is currently being prepared for final publication.

[7] National Strategy for Information Sharing (NSIS) (October 2007), p. A1-6, 7.

[8] The terms "process" and "cycle" are used interchangeably when referring to this chart in the remainder of this CONOPS.

related suspicious activities. The initiative will ensure that NSI participants at all level of government adopt consistent policies and procedures that foster broader sharing of terrorism-related SARs while ensuring that privacy and civil liberties are adequately protected in accordance with Federal, State, and local laws and regulations.

1.3 NSI Concept of Operations

This document presents a top level operational view of the NSI. Specifically, the CONOPS:

- Provides a common understanding of the NSI process so that implementation activities can be planned, executed, and measured;
- Defines the requirements that drive the NSI process and associated implementation activities;

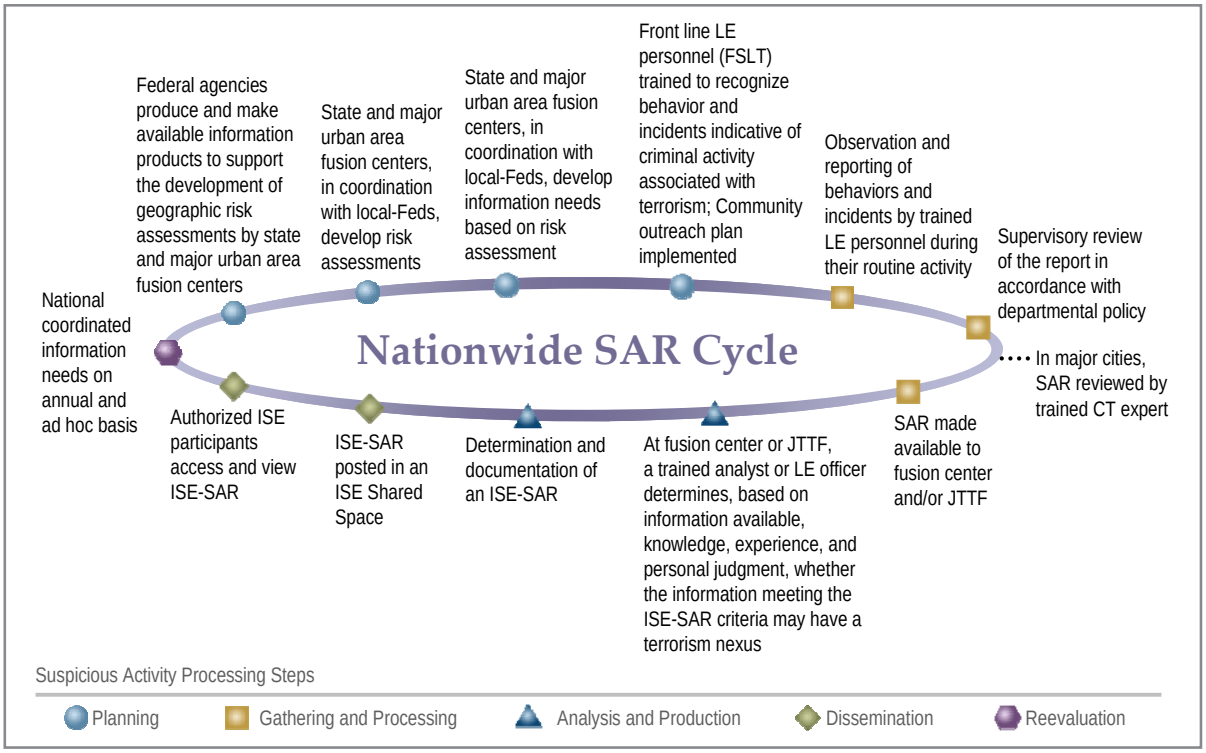

Figure 1-1. Overview of Nationwide SAR Cycle

- Describes the overall process and multiple ISE-SAR-related activities in sufficient detail to ensure that these activities adhere to standard approaches and that all embody adequate protection for privacy and civil liberties;
- Clarifies the role of the EE as a microcosm of the broader NSI—a smaller-scale implementation testbed;

- Describes the roles, missions, and responsibilities of NSI participating agencies and the top-level NSI governance structure; and
- Serves as the foundation for a number of other NSI Baseline Documents.

1.4 NSI Baseline Documents

1.4.1 ISE-SAR Functional Standard

Version 1 of the *ISE-SAR Functional Standard* was published in January 2008, and will be revised based on the results of the EE and other NSI activities.[9] The standard:

- Requires all departments or agencies that possess or use terrorism or homeland security information or operate systems that support or interface with the ISE to follow a common format for sharing ISE-SAR information;
- Provides an IEPD—consistent with the NIEM standard—that governs ISE-SAR information exchanges to include a full inventory of data classes, elements, and definitions;
- Outlines general criteria to guide law enforcement officers or analysts in determining whether a particular report has a potential terrorism nexus, i.e., one that meets the threshold for designation as an ISE-SAR; and
- Describes the ISE-SAR information flow, highlighting the filtering and decision-making steps that separate terrorism-related SARs from the large volume of unrelated information.

1.4.2 Privacy and Civil Liberties Analysis

The *ISE-SAR Functional Standard and Evaluation Environment Privacy and Civil Liberties Analysis*, issued on September 5, 2008, examines the privacy and civil liberties ramifications of the ISE-SAR Functional Standard. It describes the vision for deploying the standard in operating environments, makes recommendations to address issues identified as a result of the examination, and identifies policies and safeguards that should be implemented at the preliminary stages of this process. It will be revised as necessary based on the results of the EE and other NSI activities.[9]

1.4.3 ISE-SAR Evaluation Environment Documents

The *ISE-SAR Evaluation Environment Segment Architecture*, to be published in December 2008, establishes short term (threshold) and longer term (objective) operational outcomes for the EE. It lays the foundation for building executable operational solutions, along with associated performance goals and measures that meet or exceed EE requirements within the framework of the ISE.[9]

[9] This report is available on the PM-ISE website, www.ise.gov.

The *ISE-SAR Evaluation Environment Implementation Guide,* also planned for December 2008 publication, describes specific services and capabilities, identifies the methods for achieving the operational outcomes defined in the Segment Architecture, and defines specific information technology assets, applications and components required for implementing the ISE process in the EE. Since the *Implementation Guide* responds to the threshold outcomes described in the Segment Architecture, it serves as the preliminary Solution Architecture for the ISE-SAR EE.

1.5 Related Documents

Although not part of the formal NSI baseline, there are a number of other documents that have made important contributions to the NSI. These include:

- *The National Criminal Intelligence Sharing Plan*, published in January 2006, serves as a foundation for a number of information sharing initiatives including the NSI.[10]
- *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, a 2006 product of the Global Justice Information Sharing Initiative, defined guidelines for establishing and operating fusion centers.[10]
- Guideline 2 – Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector, approved by the President in November 2006, established a number of requirements that formed the basis for the initial ISE-SAR business process.[11]
- *Privacy Impact Assessment for the eGuardian Threat Tracking System*, completed in August 2008, describes the measures taken to ensure that the FBI's eGuardian system satisfies privacy requirements.
- *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* was formally released in November 2008 following approval by all participating organizations. This report, available at describes the all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity by the local police agencies.[10]

[10] This report is available on the Global Justice website at http://www.it.ojp.gov/default.aspx?area=globalJustice&page=1236.
[11] This report is available on the PM-ISE website, www.ise.gov.

Section 2 NSI Requirements

2.1 Overview

Suspicious activity reporting documents "observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention."[12] Examples include surveillance, photography of facilities, site breach or physical intrusion, cars parked or boats anchored in atypical locations, cyber attacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemicals or toxic materials, or other unusual behavior or incidents.

Following a thorough assessment to ensure that the information has been legally obtained and has a potential nexus to terrorism—typically involving reviews by both local authorities and officials at a fusion center or Federal agency against criteria set forth in the ISE-SAR Functional Standard—those reports determined to be terrorism-related are designated as ISE-SARs and are documented, processed, analyzed, and shared by ISE participants. Development of this unified end-to-end process for the NSI is driven by specific operational requirements set forth in the NSIS.

2.2 Operational Requirements

2.2.1 Introduction

The operational requirements for the NSI have evolved over the last several years, culminating in the publication of the NSIS in October 2007. In 2006, for example, the Guideline 2 Report cited the need to define requirements "… for reporting, tracking, and accessing suspicious incidents and activities."[13] The NSIS synthesized this work into a specific set of SAR requirements that form the basis for the development of the NSI process discussed in more detail in Sections 3 and 4.

The requirements outlined below in Sections 2.2.2 and 2.2.3 come directly from the section on Suspicious Activity Reporting in Appendix 1 of the NSIS.[14] Although the National Strategy assigns responsibility for some of these primarily to Federal Government agencies and allocates others to State, local, and tribal governments, it is clear that they need to be viewed holistically as a common set of requirements for the NSI requiring collaboration across all levels of government.

[12] ISE-SAR Functional Standard, p. 1.
[13] Guideline 2 Report, p. 18.
[14] NSIS, pp. A1-6-A1-7. Note that, although these requirements are presented in the NSIS in the context of SAR, some may also be applicable to other processes that support sharing other types of terrorism-related information.

Although not explicitly cited as a SAR requirement in Appendix 1 of the NSIS, the importance of an integrated process for managing information needs has long been recognized as a critical part of the NSI process. The main body of the NSIS highlights the need to "facilitate the exchange of coordinated sets of requirements and information needs across the Federal and non-Federal domains to help guide the targeting, selection, and reporting of terrorism-related information."[15] In addition, the ISE Implementation Plan includes a specific action to address State and local and private sector needs and priorities for terrorism information.[16] Consequently, Section 2.2.2 and the discussion of the nationwide SAR cycle in Section 4, incorporate an explicit recognition of the requirement to address information needs as part of the NSI.

2.2.2 Federal Responsibilities

As part of the NSI, the Federal Government will develop a plan and provide State and major urban area fusion centers a mechanism to gather and report locally generated information to appropriate Federal entities, other States, and localities. This locally generated information will include reports by the public or governmental personnel regarding suspicious incidents, events, and activities. Specific activities include:

1. Providing reports and awareness training to State, local, and tribal authorities regarding the strategic goals, operational capabilities, and methods of operation utilized by international and domestic terrorist organizations so that local events and behaviors can be viewed within the context of potential terrorist threats;
2. Developing a prioritized listing of the specific types of locally generated information of interest to Federal entities responsible for assessing the national threat environment and which supports the rapid identification of emerging terrorist threats;
3. Identifying resources capable of communicating and updating these information requirements to State, local, and tribal officials via State and major urban area fusion centers;
4. Establishing a unified process to support the reporting, tracking, processing, storage, and retrieval of locally generated information;
5. Ensuring that efforts to gather, document, process, analyze, and share locally generated information are carried out in a manner that protects the privacy and legal rights of Americans; and

[15] Ibid., p. 11.
[16] ISE Implementation Plan, p. 74.

6. Facilitating the exchange of coordinated sets of requirements and information needs across the Federal and non-Federal domains to help guide the targeting, selection, and reporting of terrorism-related information.[17]

2.2.3 State, Local, and Tribal Responsibilities

State and major urban area fusion centers will support the gathering of locally generated terrorism information, homeland security information, and law enforcement information related to terrorism.[18] Specific activities include:

1. Completion of a Statewide and/or regional risk assessment (threat, vulnerability, and consequence);
2. Using this assessment to identify priority information needs;
3. Identification of data sources and repositories of prioritized information;
4. Maintaining an information gathering and reporting strategy utilizing existing local capabilities;
5. Developing, implementing, and maintaining a method for communicating information priorities to local gatherers of information;
6. Ensuring that priority information, including SARs, are disseminated to and evaluated by appropriate government authorities and appropriate critical infrastructure owners and operators;
7. Ensuring that the processes and protocols for 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;
8. Identifying requirements that support a unified process for reporting, tracking, and accessing SARs; and
9. Defining a feedback mechanism.

[17] As noted above, this requirement was not part of Appendix 1 of the NSIS, but was included here because it is clearly consistent with the other Appendix 1 SAR requirements. Moreover, it provides the clearest statement of the importance of a national process supporting CT information need.

[18] Although not specifically covered in the discussion of SAR, page A1-4 of the NSIS requires Urban Area Security Initiative (UASI) fusion centers to work with State officials to determine the most effective manner in which to incorporate the UASI into the statewide information sharing framework, to include how information flows between UASIs and the fusion center designated by the governor as the primary State interface with the Federal Government.

2.3 Privacy and Civil Liberties Requirements[19]

2.3.1 Introduction

The overarching goal for the NSI is that ISE-SARs be shared to the maximum extent possible among authorized Federal and SLT law enforcement, homeland security and other ISE participants, while protecting privacy and other legal rights. Section 1016(d) of IRTPA calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the ISE. In response, Presidential Guideline 5 directed the Attorney General and the Director of National Intelligence (DNI) to develop guidelines "to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information."[20]

The resulting ISE Privacy Guidelines, approved by the President in November 2006, describe the means by which Federal departments and agencies participating in the ISE will protect privacy and civil liberties in the development and operation of the ISE.[21] The Privacy Guidelines also require Federal agencies and the PM-ISE to work with SLT governments and private sector organizations that are part of the ISE to ensure that they implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in the Guidelines.[22] Therefore, all NSI participants—both Federal and non-Federal—must adopt policies and procedures that are consistent with the ISE Privacy Guidelines.

The *ISE-SAR Functional Standard* embodies a number of features that protect privacy and other legal rights while still supporting broad dissemination of ISE-SARs and maximum sharing of the relevant information. For example, the IEPD in Section IV of the standard allows for two different data formats for exchanging ISE-SAR information. The ***Detailed Format*** includes all data elements set forth in Section IV of the ISE-SAR Functional Standard, *including* those designated as privacy fields, i.e., fields containing personal information; the ***Summary Format*** excludes these privacy fields, but includes all other data elements in the IEPD. The ability to choose between these two formats, depending on privacy laws and policies, provides a powerful mechanism for controlling access to personal information. In addition, the IEPD contains source elements that

[19] The requirements in this section are essentially a more detailed exposition of Requirement 5 in Section 2.2.2. They are described separately because of the overriding importance of protecting privacy and civil liberties in the NSI process.

[20] "Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements In Support of the Information Sharing Environment" (December 2005), Section (2) (e).

[21] Guideline 5 – Guidelines to Implement Information Privacy Rights and Other Legal Protections in the Development and Use of the Information haring Environment (November 2006). See http://www.ise.gov/docs/guidance/guideline%205%20-%20privacy%20rights%20and%20legal%20protections.pdf.

[22] Ibid., p. 10.

enforce the principle of limited retention of ISE-SAR information by enabling time-dependent purging of ISE-SARs after human review.[23]

2.3.2 Specific Privacy Requirements

In general, participating agencies must conform to the ISE Privacy Guidelines and associated implementation guidance.[24] In addition, participating agencies should review the recommendations in the *ISE-SAR Functional Standard and Evaluation Environment Privacy and Civil Liberties Analysis* and adopt them where appropriate. Specifically, agencies participating in the NSI must:

1. Demonstrate that policies, procedures, and mechanisms, consistent with the Privacy Guidelines, are in place to ensure that privacy and civil liberties are adequately protected in the gathering, documenting, processing, analyzing, and sharing terrorism-related SARs;
2. Refrain from exchanging information using the Detailed Format until these policies and procedures are in place;
3. Integrate the management of terrorism-related suspicious information with processes and systems used to manage other crime-related information and criminal intelligence, thereby leveraging existing policies and protocols that protect the information privacy, civil liberties, and other legal rights of the public;
4. Provide adequate training to all agency personnel participating in the gathering, documenting, processing, analyzing, and sharing of terrorism-related SARs;
5. Use appropriate physical, technical, and administrative measures to safeguard ISE-SAR information from unauthorized access, disclosure, modification, use, or destruction; and
6. Promote a policy of openness and transparency when communicating to the public regarding their SAR policies and procedures.

[23] ISE-SAR Functional Standard, Section IV, pp. 12-22.

[24] Supporting Guidance includes the *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment* (September 2007) and a web-based all-inclusive source of resources and tools to help ensure compliance with the ISE Privacy Guidelines. See http://www.ise.gov/pages/privacy-fed.html.

Section 3 NSI Business Process Overview

3.1 Existing ("As-Is") Process

As noted earlier, use of SARs as a crime fighting and prevention tool is not new; it has been a standard part of operating procedures for Federal, State, and local law enforcement agencies for years. Although these local processes generally worked well, they were largely *ad hoc*, centered on individual agency needs, and often depended heavily on long-established personal relationships rather than a coordinated sharing strategy. A standard approach for documenting and sharing SARs was lacking. As the *SAR Support and Implementation Project* report observed:

> There are over 17,000 local law enforcement agencies in the United States that document information regarding suspicious criminal activity including that related to terrorism. In the absence of national guidance, individual jurisdictions have independently developed intradepartmental policies and procedures for gathering and documenting SARs; however, the lack of standardization has restricted the efficient analysis and sharing of this information on a regional and/or national basis."[25]

In the Fall of 2006, an interagency working group under the auspices of the PM-ISE documented a number of SAR processes used by Federal, State, and local agencies. Although the details varied, these processes exhibited a number of commonalities. They all typically involved a local information acquisition step followed by a human review and determination prior to further dissemination. All agencies stressed the importance of this review step in weeding out reports that may appear to be "suspicious" at the local level but are resolved after a more in-depth review, perhaps including additional information available to a fusion center or Federal agency. While these individual processes served the needs of the separate organizations, they focused on the front end (gathering and processing) but neglected the critical end-to-end steps (documenting, analyzing, and sharing) required to fully address the NSIS requirements.

3.2 Objective ("To Be") Process

To address this deficiency, the PM-ISE in partnership with a number of Federal, State, and local agencies, has been working to define and implement a process that maintains the requisite degree of originator control embodied in the existing processes, but also incorporates standard approaches that support sharing terrorism-related SARs with authorized recipients across the ISE. This process has evolved over the past two years as the requirements have become better understood. It was documented in Version 1 of

[25] SAR Support and Implementation Project, p. 6.

the ISE-SAR Functional Standard in January 2008, and has since been modified to incorporate requirements not fully addressed in the initial version.[26]

The steps in the NSI cycle depicted in Figure 1-1 are presented in detail in Section 4, but first it is important to delineate some key principles that apply across the cycle:

- The process represents a cycle that responds to SAR requirements as set forth in the NSIS, including some steps (e.g., information needs, threat assessments) that are broader than the SAR process, i.e., they contribute to other ISE processes as well;
- It incorporates multiple levels of review and vetting to ensure that information is legally gathered and managed and has a potential nexus to terrorism;
- To support local agency needs and to ensure that all Federal, State, and local laws and regulations are followed, the process relies on a distributed system of sharing that maintains agency control over ISE- SAR information;
- The process is not static, but will be modified to incorporate lessons-learned and best practices from activities such as the EE;
- To foster collaboration across all levels of government, the process enables greater awareness of information needs among Federal and SLT agencies;
- Where possible, SAR handling will be incorporated into existing processes and procedures used to manage other crime-related information and criminal intelligence so as to use common policies and protocols that protect the information privacy, civil liberties, and other legal rights of the public; and
- ISE-SARs containing personal information that are later determined (either by the original submitting organization or another participating agency) to have no terrorism or criminal nexus, will be removed from ISE Shared Space and participants notified of the change in status.

Before discussing the individual steps of the process, an example may clarify overall process, the flow of information, and the decision steps involved.

3.3 Example Operational Scenario

In rural Virginia, an owner of a self-storage locker business takes his dog out for a walk on the self-storage lot. As he follows his dog he observes a U-Haul Rental Truck with a Washington, D.C. license plate and three men unloading metal drums from the rental truck and placing them in a locker. As he and his dog approach, the men quickly close the back of truck and the storage locker door and one of them tries to block his view of the license plate, but not before the man makes a quick mental note of the license number. He says hello but receives no acknowledgment from the men. The man

[26] The ISE-SAR Functional standard will be updated to incorporate these changes and the results from the EE.

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.

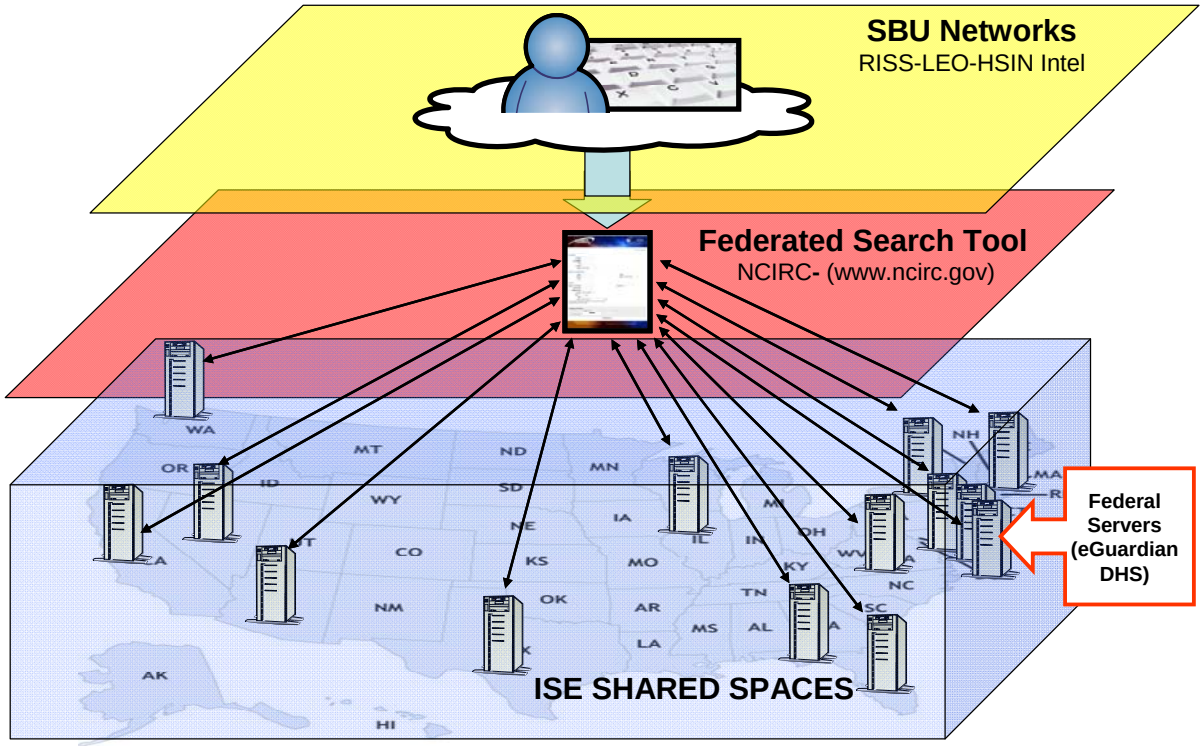

Figure 5-1. Top-level View of ISE-SAR Evaluation Environment

5.3 Functional Capabilities

The EE will provide the following capabilities to participating sites:

1. The ability for authorized organizations to format incoming SARs in accordance with the ISE-SAR Functional Standard and post the resulting reports in an ISE Shared Space;
2. The ability for authorized EE participants in fusion centers; Federal, State and local LE agencies; JTTFs; and FIGs to access and view ISE-SARs;[42]
3. The ability to store and retrieve free text SAR summaries with no personal information in a sharable library accessible by EE participants and others;[43]
4. Protected access to ISE Shared Spaces using existing networks authorized to store and transport formerly SBU information without requiring additional identification or authentication;[44]
5. Assistance in developing and improving supporting procedures and business processes as required, including privacy-related policies and procedures; and
6. Assistance in developing risk assessments and information needs to inform the gathering of terrorism-related SARs on a local or regional basis.

[42] The long term goal is that the information in ISE-SARs be usable in other tools and applications available to ISE participants. For the EE, however, ISE-SARs can only be accessed and displayed; there will be no capability to store them locally.

[43] The library was originally proposed as a "quick win" that could be implemented easily with minimal privacy impact. What, if any, long-term role it will play in the NSI is still under consideration.

[44] Although the term "SBU" is still in common use, a Presidential memorandum issued in May provided a new framework for what it defined as Controlled Unclassified Information (CUI). CUI will eventually replace the SBU designation, but the terms will be used interchangeably. See *Memorandum for the Heads of Executive Departments and Agencies: Designation and Sharing of Controlled Unclassified Information (CUI)*, White House (May 9, 2008). Available online at: http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html.

Section 6 Managing the NSI

6.1 Agency Roles, Missions, and Responsibilities

The NSI is a collaborative effort among a number of Federal and SLT government agencies with CT responsibilities. This section delineates their roles and responsibilities in the NSI.

6.1.1 Federal

1. The ***PM-ISE*** is the sponsor of the NSI pursuant to his role of "assisting in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE." [45] The office of the PM-ISE
   a. Provides broad direction, coordination, and oversight of all NSI activities;
   b. Coordinates all outreach and public affairs activities about the NSI;
   c. Reports results to the ISC and other Federal Government organizations as appropriate;
   d. Issues, maintains, and updates the ISE-SAR Functional Standard and other NSI baseline documents in consultation with the ISE-SAR Steering Committee (ISE-SSC) and the ISC;
   e. Supports Federal agencies in planning and budgeting for NSI activities; and
   f. Chairs ISE-SAR Steering Committee.
2. The ***ISE Privacy Guidelines Committee (PGC)***, a standing committee of the ISC composed of ISC member agencies' ISE Privacy Officials, provides advice and guidance to NSI participants as needed to assist them in ensuring that all NSI activities are conducted consistent with applicable laws and policies protecting privacy and civil liberties.
3. ***DOJ/OJP/BJA***
   a. Provides overall project management for major parts of the ISE-SAR EE;
   b. Executes all tasks and responsibilities described in the PM-ISE-DOJ Memorandum of Understanding, dated July 29, 2008;
   c. Provides core services for the ISE-SAR EE—federated searches and retrievals of ISE Shared Spaces.
   c. Reports regularly on progress to the PM-ISE and the ISE-SSC; and
   d. Serves as a member of the ISE-SAR Steering Committee.

[45] IRTPA, §1016(f)(2)(A).

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.

6.1.2 State, Local, and Tribal

1. ***State, local, and tribal law enforcement agencies***
   a. Train front line personnel to recognize behavior and incidents indicative of criminal activity associated with terrorism;
   b. Ensure that personnel observe and document such behaviors in accordance with laws and regulations;
   c. Review SARs for accuracy, completeness, and potential terrorism nexus; and
   d. Forward SARs to State and major urban area fusion centers (and to JTTFs where appropriate) for further analysis or action.
   e. Provides members to the ISE-SAR Steering Committee.
2. ***State and major urban area fusion centers***
   a. Train personnel to process and analyze SARs received from SLT law enforcement agencies;
   b. Demonstrate that policies and procedures are adequate to protect privacy and civil liberties;
   c. Review SARs received from SLT law enforcement agencies to determine whether they should be designated as ISE-SARs;
   d. Post all ISE-SARs in an ISE Shared Space in a manner consistent with the ISE-SAR functional standard;
   e. Develop local or regional risk assessments in collaboration with local DHS and FBI representatives;
   f. Develop information requirements based on local or regional risk assessments and national information needs; and
   g. Ensure that ISE-SAR information is accessible by the other fusion centers in the State or geographic region as appropriate.

6.2 The ISE-SAR Steering Committee

The ISE-SSC provides overall direction and oversight of the NSI. The ISE-SSC, shown in Figure 6-1, is chaired by the PM-ISE and is comprised of members from all the Federal and State, local, and tribal stakeholders participating in the NSI. It serves as a forum for:

- Ensuring that all NSI participants have a common understanding of the goals and activities of the NSI;
- Coordinating agency outreach and public affairs releases to ensure they are consistent with the goals and activities of the NSI;
- Reviewing and approving major NSI baseline documents (see Section 1.3);

- Reviewing NSI progress and making adjustment to plans and activities as required;
- Reviewing the results of the ISE-SAR EE and planning for follow-on activities and resources;
- Providing requirements to the CTISS Committee for modifications to the ISE-SAR Functional Standard and approving changes where appropriate; and
- Serving as a forum for addressing other ISE-SAR Community-wide issues of concern.

The ISE-SSC is linked to the overall ISE governance structure through the PM-ISE and the ISC.[46] In particular, given the importance of the ISE-SAR Functional Standard and privacy issues to the NSI, it has close ties to the CTISS Committee and the PGC. The ISE-SSC can establish temporary working groups to address specific issues; these groups will be disbanded when the issue is resolved. The ISE-SSC provides strategic direction and oversight to the EE, but day-to-day execution is in the hands of a project management team.

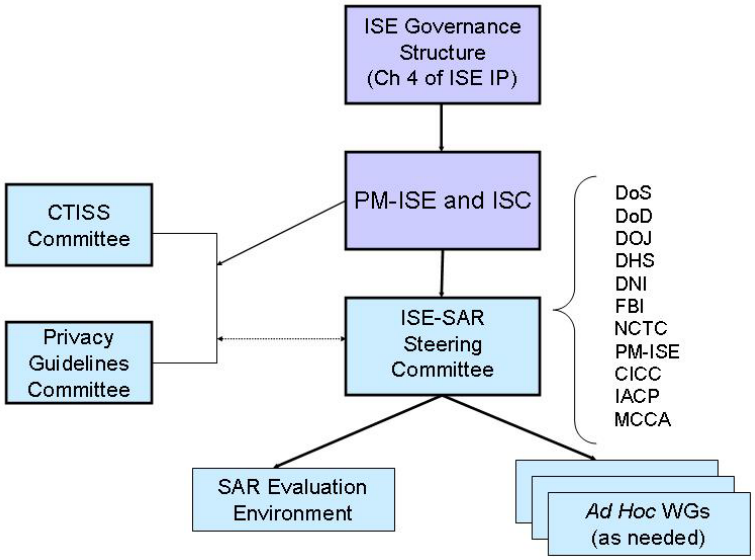

Figure 6-1. ISE-SAR Steering Committee Structure

6.3 NSI Performance Management

The long term goal for the NSI is that most Federal, State, local, tribal, and law enforcement organizations will participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity. Realizing this goal requires that specific performance goals and measures be established for the ISE-SAR EE and other NSI activities. As part of the process of

[46] ISE Implementation Plan, pp. 36-39.

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.

Appendix A – Mapping of NSIS Requirements to NSI Cycle

Table A-1 maps the NSIS requirements identified in Section 2.2 to the associated step(s) in the NSI cycle described in detail in Section 4 and to the steps in the information flow description in Part C of the ISE-SAR Functional Standard. Since Version 1 of ISE-FS-200 dealt primarily with the parts of the overall process from initial observation through sharing and use, some of the NSIS requirements have no direct mapping and are denoted as N/A in the ISE-FS-200 column of the table. As noted earlier, ISE-FS-200 will be updated based on the EE and other NSI activities.

Table A-1. Mapping of NSIS Requirements to the NSI Cycle and the Functional Standard

Reference	NSIS Requirement	NSI Cycle[47]	ISE-FS-200 Ver. 1[48]
Federal Responsibilities			
2.2.2.1.	Providing reports and awareness training to State, local, and tribal authorities regarding the strategic goals, operational capabilities, and methods of operation utilized by international and domestic terrorist organizations so that local events and behaviors can be viewed within the context of potential terrorist threats	Section 4.1.1	Step 8
2.2.2.2.	Developing a prioritized listing of the specific types of locally generated information of interest to Federal entities responsible for assessing the national threat environment and which supports the rapid identification of emerging terrorist threats	Section 4.5.1	N/A
2.2.2.3.	Identifying resources capable of communicating and updating these information requirements to State, local, and tribal officials via State and major urban area fusion centers	Sections 4.1.3, 4.5.1	N/A
2.2.2.4.	Establishing a unified process to support the reporting, tracking, processing, storage, and retrieval of locally generated information	Sections 4.1.4 - 4.4.2	Steps 1-5
2.2.2.5.	Ensuring that efforts to gather, process, analyze, and store locally generated information are carried out in a manner that protects the privacy and legal rights of Americans	Sections 4.1.4 - 4.4.2	Steps 1-5
2.2.2.6.	Facilitate the exchange of coordinated sets of requirements and information needs across the Federal and non-Federal domains to help guide the targeting, selection, and reporting of terrorism-related information	Sections 4.1.3, 4.5.1	N/A
State and Local Responsibilities			
2.2.3.1.	Completion of a Statewide and/or regional risk assessment (threat, vulnerability, and consequence)	Section 4.1.2	N/A

[47] The references are to specific subsections of Section 4 of this CONOPS.
[48] The references are to the steps described in the table on pages 29-32 of the *ISE-SAR Functional Standard*.

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