# Nationwide Suspicious Activity Reporting Initiative (NSI)

## Technical Implementation Options

Prepared by the Office of the
Program Manager, Information Sharing Environment

March 2010

# NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE (NSI)

# TECHNICAL IMPLEMENTATION OPTIONS

**Prepared by the Office of the**
**Program Manager, Information Sharing Environment**

Version 1
March 2010

# TABLE OF CONTENTS

**1 Introduction ..... 1**

**1.1 Background ..... 1**

**1.2 Purpose ..... 2**

**2 NSI Technical Implementation Considerations ..... 2**

**2.1 General Approach ..... 2**

**2.2 ISE-SAR Functional Standard ..... 3**

**2.3 ISE Shared Spaces ..... 3**

**3 NSI Shared Space Implementation Options ..... 4**

**3.1 Locally-Based Server Option ..... 4**

3.1.1 General description ..... 4

3.1.2 Data Entry Methodology ..... 5

3.1.3 Vetting Area ..... 6

**3.2 Service Provider Option Through eGuardian ..... 6**

3.2.1 General description ..... 6

3.2.2 Data Entry Methodology ..... 6

3.2.3 Vetting Area ..... 7

**4 Summary ..... 7**

# 1 Introduction

## 1.1 Background

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort among Federal and State, local, and tribal (SLT) government agencies with Counterterrorism (CT) responsibilities. Developed pursuant to Presidential direction, it establishes a nationwide capability to gather, document, process, analyze, and share information about suspicious incidents to enable rapid identification and mitigation of potential terrorist threats.[1] The resulting NSI business process (often referred to as the NSI cycle) was described by the Program Manager for the Information Sharing Environment (PM-ISE) in a Concept of Operations for the NSI published in December 2008 and in a revised functional standard in May 2009.[2]

The NSI 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 replicable process whereby SAR information can be shared to help detect and prevent terrorism-related criminal activity. Although it did not specifically use 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 due to what the Commission referred to as "the human or systemic resistance to sharing information." The Commission recognized that Federal and SLT governments have access to information which, when synthesized with information from other sources, could help identify precursor activities of terrorist attacks. 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 privacy, civil liberties, and other legal rights are adequately protected.

The PM-ISE developed and documented the NSI process in conjunction with the Department of Justice, Bureau of Justice Assistance (DOJ/BJA); the Federal Bureau of Investigation (FBI); the Departments of Homeland Security and Defense (DHS and DoD); the Office of the Director of National Intelligence (ODNI); and state and local law enforcement agencies from across the nation. In addition, a number of major law enforcement organizations—the Criminal Intelligence Coordinating Committee (CICC), the International Association of Chiefs of Police (IACP), the Major City Chiefs Association (MCCA), the National Sheriffs Association, and the Major County Sheriffs Association—have formally endorsed the NSI and have been key players in the effort.

Over the last two years, these organizations collaborated on an ISE-SAR Evaluation Environment (ISE-SAR EE) at a number of Federal and SLT agencies across the country to test, evaluate, and hone the policies, procedures, and technology concepts needed to implement a unified process for gathering, documenting, processing, analyzing, and sharing SARs that are deemed to be reasonably indicative of potential intelligence gathering or pre-operational planning related to terrorism or other criminal activity.

[1] *The National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (October 2007). pp. A1-6 available at http://www.ise.gov/pages/documents.aspx.

[2] The *NSI Concept of Operations, Version 1* (December 2008) and *ISE-FS-200, Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.5* (May 21, 2009) are both available at http://www.ise.gov/pages/sar-initiative.aspx.

As part of the EE, the stakeholders implemented a technology-independent federated search capability that enables state and local law enforcement analysts to view ISE-SARs gathered by other federal, state and local authorities allowing law enforcement agencies to quickly obtain and use information from other jurisdictions to support counterterrorism operations. This capability provides broad visibility into local events, enabling the identification of regional and national patterns and trends indicative of emerging threats (both terrorism and potentially those involving other types of criminal activity).[3]

On December 17, 2009 the White House conferred the responsibility for NSI implementation on the DOJ.[4] A new NSI Program Management Office (PMO) has been established to build on the lessons learned and best practices from the Evaluation Environment related to business processes, training, privacy and civil liberties, and technology concepts. Moving forward, all participants in the NSI must implement the following:

1. Privacy and Civil Liberties policies and procedures consistent with the ISE Privacy Guidelines;[5]

2. A multi-level vetting process consistent with the process described in the NSI CONOPS;

3. Training of frontline officers, analyst and executives; and

4. Appropriate technology to support the NSI business process that is compliant with the ISE-SAR Functional Standard.

### 1.2 Purpose

The purpose of this paper is to provide guidance to participating agencies in choosing the technology implementation option best suited to their individual local operational and technical situations. It briefly describes the two available technical implementation options. While both are based on the ISE Shared Spaces concept, support the NSI business process, and adhere to the ISE-SAR Functional Standard, the two implementation methods have different requirements that agencies must address to ensure proper connectivity to, and effective utilization of, the NSI environment.

## 2 NSI Technical Implementation Considerations

### 2.1 General Approach

The major objective of the NSI is to establish—at each of the participating sites—policies and business processes that support the gathering, documenting, processing, analyzing, and sharing of SARs while ensuring that privacy and civil liberties are adequately protected in

[3] Although the ISE-SAR Evaluation Environment focused exclusively on SARs that were reasonably indicative of criminal activity associated with terrorism, one of its key findings was that the NSI should be expanded to encompass information on other potential crimes as well as terrorism, i.e., to become an "all-crimes" environment.

[4] Memorandum from the Assistant to the President for Homeland Security and Counterterrorism entitled "Strengthening Information Sharing with the Establishment of Two program Management Offices" (December 17, 2009).

[5] See http://www.ise.gov/pages/privacy-implementing.aspx for the ISE Privacy Guidelines and related material.

accordance with Federal, State, and local laws and regulations. Overall, NSI implementation is grounded on the premise that—depending on available technology and the needs of the individual participating agencies—there will always be multiple technical implementations that can achieve this objective. Moreover, these implementations will change over time as new capabilities become available and old ones are replaced. Consequently, NSI implementation must always accommodate different technical approaches; it can never be a "one size fits all" effort. To achieve this general approach, two primary unifying capabilities that allow different implementations to freely exchange SAR information are necessary: 1) the common adoption of the ISE-SAR Functional Standard and 2) the concept of ISE Shared Spaces.

## 2.2 ISE-SAR Functional Standard

This standard, issued as part of the PM-ISE's Common Information Sharing Standards (CISS) program, describes a uniform process and associated data model to support the identification, documentation, and sharing of ISE-SAR information to the maximum extent possible consistent with the protection of privacy, civil rights, and civil liberties. The standard serves as the unifying glue that allows participating agencies with different technical implementations and systems to exchange information effectively and efficiently. It provides the ability for different technical implementations to represent details about terrorism-related suspicious activity in a standard exchange format to help facilitate the identification of useful investigatory or trending information.

The *ISE-SAR Functional Standard* describes a multilevel review process—originally set forth in the NSI Concept of Operations—for identifying those SARs with a potential nexus to terrorism out of the thousands of suspicious activities documented by source agencies each day.[6] Following the "gathering" step and a preliminary review by a local agency, a trained analyst or law enforcement officer at a fusion center or Federal agency first determines whether the suspicious activity meets any of the criteria set forth in Part B of the *ISE-SAR Functional Standard*. These criteria describe behaviors and incidents identified by law enforcement officials, counterterrorism experts, and privacy and civil liberties advocates across the country as being indicative of criminal activity associated with terrorism. Following this, the analyst or officer then determines—based on a combination of knowledge, experience, other available information, and ultimately personal judgment—whether the information is reasonably indicative of criminal activity related to terrorism. If this determination is made, the report is then documented in the data format and schema prescribed by the standard's Information Exchange Package Document (IEPD) and made available to all appropriate ISE participants through ISE Shared Spaces in accordance with the requirement of the NSI Privacy, Civil Rights, and Civil Liberties Framework.

## 2.3 ISE Shared Spaces

An ISE Shared Space is a technology concept whereby terrorism information, as defined in a CISS-issued functional standard, is made available by one ISE participant to other agencies. An ISE Shared Space consists of hardware and software that support a participant's policies and business processes for a particular ISE activity. There may be multiple ISE Shared Spaces

[6] This process is described on pages 7-11 of the ISE-SAR Functional Standard and on pages 12-19 of the NSI CONOPS. (See Footnote #2 for full citation.)

under the management, control, and resourcing responsibility of an ISE participant. This responsibility includes ensuring that information security, data integrity, use, retention, and other technology-related data stewardship requirements are met; in other words, that the ISE Shared Space technical capability supports established ISE mission processes.

A detailed discussion of the ISE Shared Spaces concept is contained in Appendix F of the ISE Profile and Architecture Implementation Strategy (PAIS)[7]. Additionally, Chapter 5 of the ISE PAIS presents a case study of one specific ISE Shared Space implementation as an illustration of how an agency might implement an ISE Shared Space as part of the NSI.

# 3 NSI Shared Space Implementation Options

There are currently two options that an NSI participant may use to implement its ISE Shared Space as part of the NSI.

1. Installing a locally-based server or web service; or

2. Using a service provider (i.e., the FBI's eGuardian system).

Although they are based on different designs, both options allow analysts to review information, format selected information in accordance with the ISE-SAR Functional Standard, and share information through ISE Shared Spaces. The two approaches are depicted in Figure 1 and discussed in more detail below.

## 3.1 Locally-Based Server Option

### 3.1.1 General description

The process established for the ISE-SAR EE featured a distributed environment consisting of individual ISE Shared Space servers at participating agency locations, consistent with the *ISE Enterprise Architecture Framework* and *ISE Profile and Architecture Implementation Strategy*.[8] Under this approach, information loaded into the ISE Shared Space servers is searched, accessed, and displayed by all authorized ISE investigative and analytic personnel to support their CT missions.[9] However, the information remains under the local control of the participating agency, i.e., the originating organization is the only one that can update a record.

[7] *Information Sharing Environment Profile and Architecture Implementation Strategy, Version 2.0* (June 2009), available at http://www.ise.gov/docs/eaf/ISE-PAIS_V2.0.pdf.

[8] Both documents are available at http://www.ise.gov/pages/eaf.aspx.

[9] *NSI Concept of Operations*, section 4.4.2.

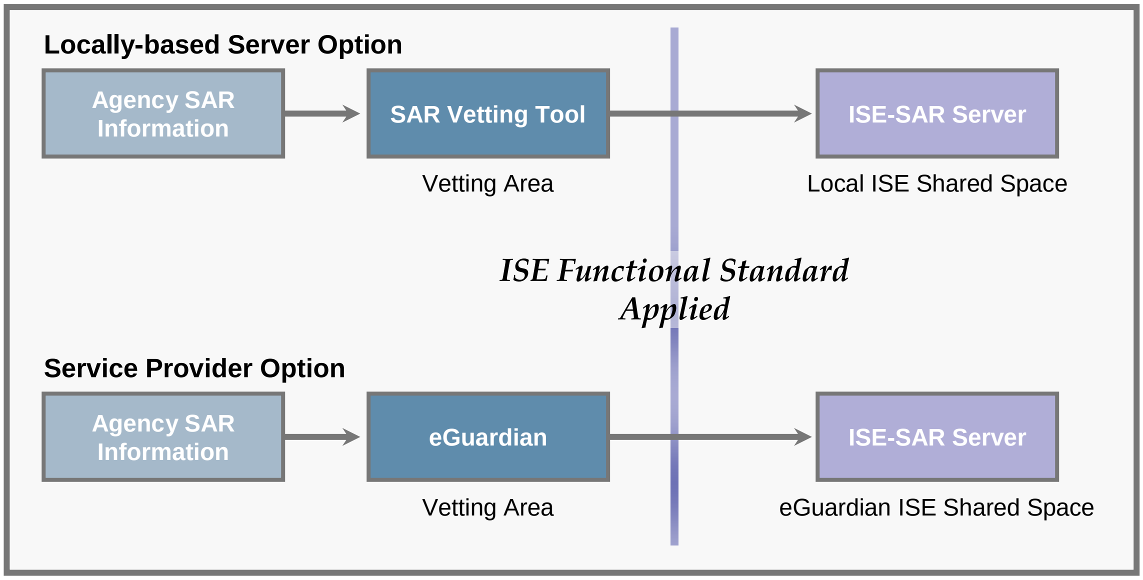


*Figure 1. NSI Implementation Options*

Agencies are required to develop a process for placing reports in ISE Shared Space that ensures that the reports are formatted in accordance with the ISE-SAR Functional Standard's IEPD.[10] Completing an agency's implementation involves two steps:

1. A fact finding and strategy formulation step to evaluate the site, describe applicable site business processes, and agree on the terms and conditions of the implementation; and

2. A second step to procure and install hardware and software, transform legacy data into a standard format, and store it (after vetting) on the ISE Shared Space server.

Based on experience during the EE, the first step typically takes three to four weeks; the second step, which may have process and policy prerequisites, spans about six weeks.

### 3.1.2 Data Entry Methodology

On a regularly scheduled (daily, hourly, etc.) basis, previously reviewed electronic data is transferred from the agency's local database to an ISE Shared Space. Prior to storing that data in an ISE Shared Space database, the data must be processed (by an Extract, Translate and Load [ETL] program) to reformat the existing data into an XML schema that satisfies the *ISE-SAR Functional Standard* requirements. The new formatted record is then stored on the server and made available to authorized users for sharing within the ISE.

In addition to entering information in the local ISE Shared Space Server, a site using the Locally-Based service option will—where it is able to determine that a reported activity is more than suspicious and has a clear connection to a likely terrorist-related crime—automatically forward selected ISE-SARs directly to e-Guardian for assessment/action by a Joint Terrorism task Force (JTTF).

[10] *ISE-SAR Functional Standard, Version 1.5* (May 2009), Sections IV and V, pp. 13-28.

### 3.1.3 Vetting Area

Depending on local requirements, ISE-SAR EE participants have adopted different approaches for gathering and storing SAR related information. Most of the sites decided to collect and vet their SAR information in a location separate from their local records systems and sources. The ISE-SAR EE team worked with these sites to create a separate data repository for SAR information (commonly referred to as a “swimming pool”). In addition, a piece of software known as the SAR Vetting Tool (SVT) allows analysts to review the data in the swimming pool and select those reports deemed to be reasonably indicative of criminal activity associated with terrorism (see Vetting Area in Figure 1). These records are then converted into the ISE-SAR Functional Standard IEPD format and transferred to the local Shared Space server where they are accessible by other participating agencies through ISE Shared Spaces. Much of the SVT software is common across all installations, but portions of it are tailored to the needs of individual sites.

## 3.2 Service Provider Option Through eGuardian

### 3.2.1 General description

The second implementation approach used during ISE-SAR EE was a Service Provider option through the FBI’s eGuardian system that was developed to enable federal, state, local, and tribal agencies to better share terrorism-related SARs. The DoD, for example, has elected to enter its Force Protection SARs into eGuardian. Some state, local, and tribal agencies who have expressed interest in participating in the NSI in the future are considering the use of eGuardian as well. eGuardian uses a centralized database and associated tools to both support JTTFs in assessing and investigating terrorism-related crimes and improve sharing of terrorism information between JTTFs and local agencies. In addition to being stored in the internal eGuardian database, ISE-SAR Information entered into eGuardian can be replicated into the eGuardian ISE-Shared Space server and made available to authorized NSI participants. The eGuardian Shared Space server allows its information to be shared with other NSI participants in ISE-SAR IEPD format.

### 3.2.2 Data Entry Methodology

Data may be entered into eGuardian in several ways: manually; through a webpage interface; using an Extract, Translate and Load program; or—as in Section 3.1.2—directly from a locally-based ISE Shared Space server. As soon as trained analysts at a fusion center affirm that the observed behavior is “reasonably indicative” of terrorism-related activity (per the ISE-SAR Functional Standard), it is made available to all authorized eGuardian users. Furthermore, this information is pushed to the eGuardian Shared Space server for other NSI participants to view. Federal, state, local, and tribal agencies and FBI field offices also post eGuardian information such as assessments of potential terrorist threats and terrorist incidents. This information is recorded, tracked and analyzed by the FBI, and—if it crosses the threshold for an assessment or investigation—assigned to one of the 106 Joint Terrorism Task Forces around the country for further action.

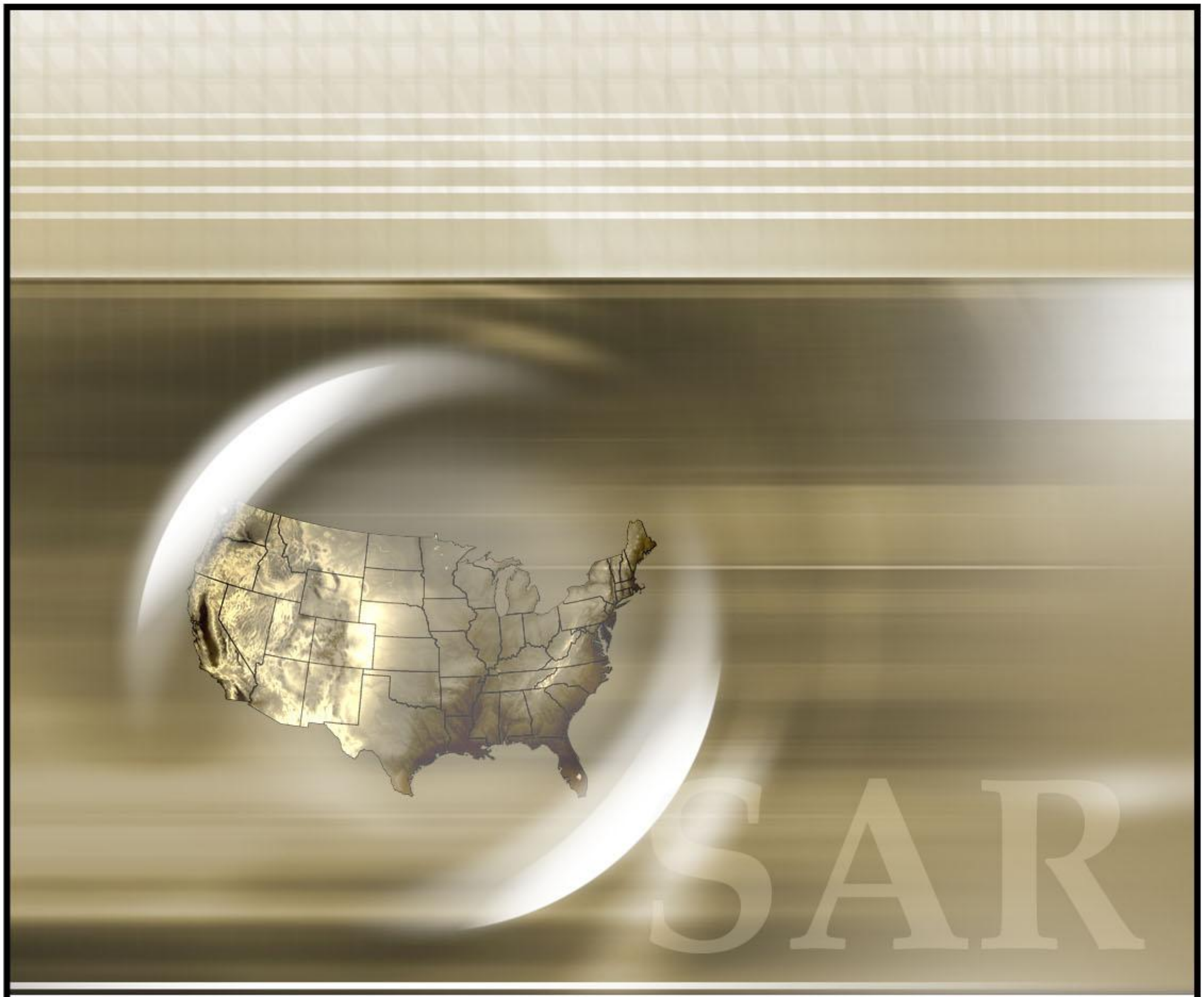
### 3.2.3 Vetting Area

Information entered into eGuardian directly by a state or local law enforcement agency may initially be viewed only by authorized users at the source organization. Once the information is entered in eGuardian, the SLT agency would then have it reviewed by a local supervisor. If approved, the information would then be forwarded to the agency's designated fusion center for formal vetting per the ISE-SAR Functional Standard. If the SAR information is determined by the fusion center to have met the criteria in the ISE-SAR Functional Standard, then it is made available to be viewed by the larger eGuardian community including the JTTFs. In addition, it is converted from the internal eGuardian format to the ISE-SAR IEPD and stored in the eGuardian ISE Shared Space server where it is accessible by all authorized NSI participants.

# 4 Summary

The goal of the NSI is to institute a unified nationwide process for gathering, documenting, processing, analyzing, and sharing SARs that are deemed to be reasonably indicative of potential intelligence gathering or pre-operational planning related to terrorism or other criminal activity. To support this unified process, the NSI incorporates a technology-independent federated search capability that enables state and local law enforcement analysts to share and view ISE-SARs gathered by other federal, state and local agencies. This capability provides broad visibility into local events, enabling the identification of regional and national patterns and trends indicative of emerging threats (both terrorism and potentially those involving other types of criminal activity

This paper provides initial guidance to help participating agencies start the process of choosing the technology implementation option best suited to their individual local operational and technical situations. It describes the general approach to implementation and explains the roles played by the ISE-SAR Functional Standard and the concept of ISE Share Spaces. It goes on to briefly describe the two technical implementation options currently in use. Although both of these options support the NSI business process, are based on the ISE Shared Spaces concept, and adhere to the ISE-SAR Functional Standard, each implementation method has unique requirements that agencies must address to ensure proper connectivity to and effective utilization of the NSI environment.



Office of the Director of National Intelligence
Attention: Program Manager, Information Sharing Environment
Washington, D.C. 20511

(202) 331-2490

Visit us on the web at http://www.ise.gov

PM-ISE