NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

STATUS REPORT

Prepared by the
Program Manager, Information Sharing Environment (PM-ISE)

February 2010

NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

STATUS REPORT

Prepared by the
Program Manager, Information Sharing Environment (PM-ISE)

February 2010

TABLE OF CONTENTS

Introduction 1

Key Findings 3

1. A Clear, Positive Impact On Local Counterterrorism Efforts 3
2. It is Possible to Combat Terrorism While Protecting Privacy 3
3. Inter-Agency Sharing of ISE-SARs Continues to Show Potential 4
4. The NSI Process is Applicable to an All-Crimes Environment 5

Background 6

Lessons-learned 9

1. Executive Leadership is Essential 9
2. NSI Implementation Must Leverage Existing Processes and Procedures 9
3. Personal Relationships are Key When Introducing New Processes 10
4. An Effective Training Program is a Critical Element of Success 11
5. Threat Information and Tactical Risk Assessments Should Drive State and Local Information Needs 12
6. Functional Standards Enable Effective Sharing of ISE-SARs 14
7. Sharing Must be Accomplished in a Way that Protects Privacy, Civil Rights, and Civil Liberties 15
8. Outreach and Collaboration with Community Leaders is Essential 17

Recommendations 18

1. Establish a Program Management Office to Manage and Oversee NSI Implementation 18
2. Apply a Robust Framework to Protect Privacy, Civil Rights, and Civil Liberties 18
3. Tailor Federal Information Products for Use by State, Local, and Tribal Agencies 18
4. Institutionalize the NSI Risk Assessment Process 19
5. Extend the NSI Process to an All Crimes Mission Environment 19
6. Formalize NSI Feedback Mechanisms 19
7. Incorporate ISE-SARs into the Broader Analytic Process 19
8. Establish Training for Mid-level Managers 20
9. Establish a Performance Measurement Plan for NSI Implementation 20

APPENDICES

Appendix A - References **21**

Appendix B - Acronyms and Abbreviations **23**

Introduction

> *"Law enforcement has excellent information gathering techniques and skills in place. However, in order for that information to be useful, it must be shared. Simply put, the heart of this initiative is to glean information from routine police work for the fusion centers so that they may provide the analysis and intelligence that is critical to our efforts against crime and terrorism."*
>
> ***- Commissioner Gerald Bailey, Florida Department of Law Enforcement***

This status report on the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) provides a summary assessment of the ISE-SAR Evaluation Environment over the last two years, highlighting four key findings and identifying a number of valuable lessons-learned. The report also provides specific recommendations to help guide the broader NSI implementation as it begins in 2010.

Over the last two years, federal, state, and local organizations have developed, tested, and evaluated the policies, procedures, and technology concepts needed to implement a unified process for gathering, documenting, processing, analyzing, and sharing suspicious activity reports that are determined to be reasonably indicative of criminal activity associated with terrorism. The Evaluation Environment provided a controlled environment where agencies could evaluate potential solutions to operational challenges and identify best practices to be incorporated as part of a broader nationwide implementation. Although the Evaluation Environment period drew to a close at the end of Fiscal Year 2009, the operational process established at the participating agencies remains in place and sites continue to share ISE-SARs on a regular basis as part of the NSI. Additional sites are already being incorporated into the process even as the plans for a full nationwide implementation are developed.

This report provides an overview of the results of the Evaluation Environment as of November 2009. In addition, two related reports will be issued in early 2010:

1. The Program Manager for the Information Sharing Environment (PM-ISE)—in consultation with the Civil Liberties and Privacy Office of the Director of National Intelligence (DNI), the Office of Privacy and Civil Liberties of the Department of Justice (DOJ), and the Legal Issues Working Group of the ISE Privacy Guidelines Committee (PGC)—is preparing an updated *NSI Privacy, Civil rights, and Civil Liberties Analysis* that provides a more detailed view of this critical aspect of NSI implementation, and
2. The PM-ISE and the DOJ Bureau of Justice Assistance (BJA), with input from state and local law enforcement, fusion center personnel, and community advocates, are developing guidance for local law enforcement and fusion centers on developing trust relationships with community representatives based on the lessons-learned from the *Building Communities of Trust* initiative. This initiative aims to build bridges and mutual understanding among community groups, local

law enforcement agencies, and state and major urban area fusion centers as a way of better protecting our local communities. The outcome is for law enforcement officers, public safety personnel, community leaders, and citizens to be better able to distinguish between innocent cultural behaviors and behavior indicative of criminal activity; and for local communities to play a more supportive role in combating terrorism-related crime. This effort is discussed in more detail in the Lessons-Learned section of this report.

Appendix A provides a comprehensive list of documents relating to the NSI.

Key Findings

After SAR training had been conducted at one of the evaluation environment agencies, the site passed on information to local police departments on how to recognize and report SARs to the fusion center for further vetting. One department—not directly involved in the ISE-SAR Evaluation Environment—received a tip submitted by a member of the public that previously might have been ignored. Because the police department had received training on how to identify and report potential terrorism-related suspicious activity the information was sent directly to the Fusion Center for further review. Fusion Center analysts vetted the information, determined that it did have a potential nexus to terrorism, and forwarded the information. That would not have otherwise gone, to the Joint Terrorism Task Force (JTTF). The information provided a key link in an ongoing JTTF investigation.

The major results from the ISE-SAR Evaluation Environment can be summarized in the following four key findings.

1. *A Clear, Positive Impact On Local Counterterrorism Efforts*

The ISE-SAR Evaluation Environment demonstrated the value of a standardized SAR process in supporting the counterterrorism efforts of state and local law enforcement agencies.

The NSI cycle includes specific steps that better enable local law enforcement agencies to leverage knowledge provided by the Federal Government on terrorist tactics, techniques, and plans. This knowledge is then used to improve training provided to frontline officers, investigators, and analysts so they are better able to recognize behaviors and incidents indicative of terrorism-related criminal activity. There are examples from Evaluation Environment sites where the proper submission of a SAR led to investigations, arrests, prosecutions, or informant recruiting.

2. *It is Possible to Combat Terrorism While Protecting Privacy*

The ISE-SAR Evaluation Environment showed that it is possible to combat terrorism effectively and protect privacy, civil rights, and civil liberties. Moreover, it reinforced the principle that local implementation of a uniform NSI Privacy, Civil Rights, and Civil Liberties Framework is critical to successful NSI implementation and provides a national benefit.

All participants in the ISE-SAR Evaluation Environment were required to implement a robust, all-inclusive approach for maximizing the protection of privacy, civil rights, and civil liberties before being allowed to share or access ISE-SAR information. The

requirements underlying this NSI Privacy, Civil Rights, and Civil Liberties Framework evolved over the course of the Evaluation Environment.[1] They include:

a. The NSI process at each participating agency must be conducted under statutory authorities and departmental privacy and civil liberties policies and procedures that are consistent with the ISE Privacy Guidelines.[2] Each participating agency must submit privacy and civil liberties policies and procedures for review to ensure consistency with the ISE Privacy Guidelines prior to sharing personal information (i.e., privacy fields) to the ISE Shared Space.

b. Implementation must include training of front line officers, investigators, analysts, and supervisors regarding the behaviors and indicators of terrorism related criminal activity.

c. Each participating agency must put in place a formal, multi-layered vetting process in which each SAR is reviewed by a supervisor and an experienced investigator or analyst specifically trained in counter-terrorism issues before it is designated as an ISE-SAR.

d. Sites should engage in outreach and collaboration at a local level with privacy and civil liberty advocacy groups.

Although participating agencies found the implementation of this Framework to be a formidable undertaking, they agreed that the NSI process could be implemented practically while still maintaining required privacy, civil rights, and civil liberties protections. Adoption of the NSI Privacy Framework as a foundation of the nationwide implementation should engender public trust by ensuring that participating law enforcement agencies across the country adopt standard processes, policies, and procedures for protecting privacy, civil rights, and civil liberties that are at least as comprehensive as those required for federal agencies by the *ISE Privacy Guidelines*.[3]

3. *Inter-Agency Sharing of ISE-SARs Continues to Show Potential*

Indications from ISE-SAR Evaluation Environment participants and other sources suggest that the sharing of SAR information between neighboring localities and within regions improves their ability to identify trends indicative of terrorism-related criminal activity. It is also likely that, under a certain set of conditions, the ability of DHS and Federal Bureau of Investigation (FBI) analysts to search local repositories would be beneficial as well. Because of the unanticipated length of time it took to ensure the NSI Privacy Framework was in place, there was a relatively short timeframe during which sites were able to operationally share ISE-SAR information across

1 Throughout the remainder of this document, the term "NSI Privacy, Civil Rights, and Civil Liberties Framework" is normally abbreviated to "NSI Privacy Framework."

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

3 The ISE Privacy Guidelines and related implementation guidance can be found at http://www.ise.gov/pages/privacy-implementing.aspx.

agencies. Nevertheless, although it was not possible to quantitatively evaluate this aspect of the SAR process, qualitative evidence gathered in discussions with participants supports the conclusion that interagency sharing will ultimately prove useful.

Agencies participating in the ISE-SAR Evaluation Environment were not authorized to share SAR data with other sites until they had met the requirements of the NSI Privacy Framework. The unanticipated length of time required to develop and implement privacy policies and procedures as part of the Framework limited the period during which most sites were able to share ISE-SARs to a few months at most. This turned out to be too short a period to amass sufficient data to quantify the value of sharing regionally and nationally. However, based on the experience of several sites that demonstrated expanded intra-regional sharing during the Evaluation Environment, the consensus view is that the ability to conduct predicated searches at regional and national levels will ultimately enhance the national capability to identify patterns and trends indicative of terrorism activity or other criminal activity associated with terrorism.

4. The NSI Process is Applicable to an All-Crimes Environment

Though the focus of the ISE-SAR Evaluation Environment is sharing terrorism-related suspicious activity, the standardized approach can apply to all types of crime.

The ISE-SAR Evaluation Environment was focused on SARs indicative of terrorism-related crimes; but both the steps in the NSI cycle and the data elements in the ISE-SAR Functional Standard are directly applicable or can be easily adapted to other types of criminal behavior. Almost all of the participating Evaluation Environment sites already operate in an "all crimes" environment where terrorism is only one of a number of criminal behaviors to which gathering and sharing of SARs may be applicable. In fact, many participating agencies noted that the standardized NSI process enhanced their ability to gather, document, process, analyze, and share other types of criminal information as well. In particular, the process may be especially effective for gang and drug-related crimes. Some additional steps will be necessary to incorporate additional suspicious behavior types, to include:

a. Changes to the NSI CONOPS and the ISE-SAR Functional Standard; and
b. Review of the privacy, civil rights, and civil liberties policies and procedures developed for the Evaluation Environment to ensure they are applicable in an all-crimes environment.

These qualifications notwithstanding, applying the NSI process to other types of criminal activities should be considered part of the logical progression for the nationwide implementation.

Background

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. It was developed pursuant to Presidential direction to establish a nation-wide capability to gather, document, process, analyze and share information about terrorism-related suspicious incidents to enable rapid identification and mitigation of potential terrorist threats.[4] The resulting process—usually referred to as the "NSI process" or the "NSI cycle"—is shown in Figure 1.

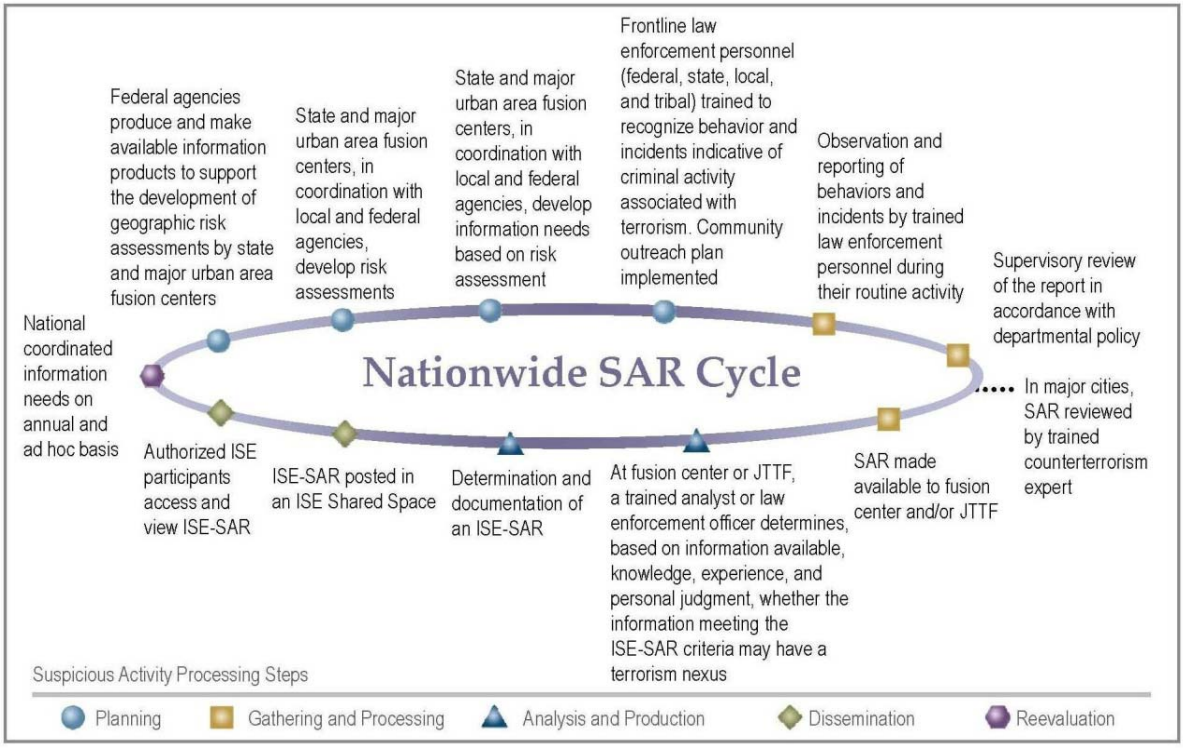

Figure 1. The Nationwide SAR Cycle

The NSI is collaboration among a number of stakeholders including the PM-ISE; DOJ and its components (in particular BJA and the FBI); the Departments of Homeland Security (DHS) and Defense (DoD); the Office of the Director of National Intelligence (ODNI); and state and local law enforcement officials from across the nation. In addition, a number of major law enforcement organizations—the Global Justice Criminal Intelligence Coordinating Council (CICC), the International Association of Chiefs of

[4] *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (October 2007), pp A1-6,7 available at http://www.ise.gov/pages/documents.aspx

Police (IACP), the Major City Chiefs Association (MCCA), the National Sheriffs Association, and the Major County Sheriffs Association (MCSA)—formally endorsed the NSI and were key players in the effort to plan and carry out the ISE-SAR Evaluation Environment.

The major objective of the ISE-SAR Evaluation Environment was to establish, at each of the participating sites, policies and business processes that support the gathering, documenting, processing, analyzing, and sharing of SARs while also ensuring that privacy, civil rights, and civil liberties were adequately protected in accordance with federal, state, and local laws and regulations. As a condition of participation, agencies were required to implement the NSI Privacy Framework that included a requirement to train all involved personnel before posting or accessing ISE-SARs.

The PM-ISE developed a performance measurement implementation plan to gauge the effectiveness of the Evaluation Environment that included a set of discrete measures designed to assess the performance of the NSI process and associated technical solutions. The plan employed a number of techniques to collect information, including automated tools, interviews, and survey reporting by the sites, and will serve as the basis for a more permanent performance measurement plan to support nationwide implementation.

Although not all sites were able to report data for all of the measures, the plan did provide a common understanding of what was being evaluated, the reporting process, and individual responsibilities. Sites provided qualitative or quantitative results that indicated the potential utility of the NSI process to broader counterterrorism outcomes, including data on:

- Federal investigations initiated as a result of SARs;
- Local investigations initiated as a result of SARs;
- Local or federal investigations that led to arrests or convictions in cases involving SARs; and
- SARs used for critical infrastructure protection and that contributed to analytic products.

Twelve state or local and three federal agencies ultimately participated in the Evaluation Environment.[5] During the period covered by this report, not all participants were able to fully share SAR data because of the unanticipated length of time needed to satisfy NSI Privacy Framework requirements. As a result, there is now a better understanding of the required level of commitment and time required before full sharing can take place. As

[5] The state or local agencies were the Boston Police Department (PD), Chicago PD, Florida Department of Law Enforcement, Houston PD, Las Vegas Metropolitan PD, Los Angeles PD, Metropolitan (Washington) DC PD, Miami-Dade Fusion Center, New York State Intelligence Center, Arizona Counter Terrorism Information Center, Seattle Police Department and the Virginia Fusion Center. FBI participated through its eGuardian system; DHS shared Federal Air Marshal Service (FAMS) data; and DoD also used eGuardian support of its Force Protection mission.

noted in the “Introduction” section of this report, the Evaluation Environment was formally concluded at the end of September 2009. But the operational process remains in place and sites continue to share ISE-SARs on a regular basis. Additional sites are already being incorporated into the process even as the plans for a full nationwide implementation are developed.

The Evaluation Environment identified a number of valuable lessons-learned that, in turn, helped generate best practices to be followed as part of the follow-on implementation of a nationwide process for SAR. The remainder of this report examines these lessons-learned and outlines specific recommendations to help guide the nationwide implementation effort beginning in 2010.

Lessons-learned

At one participating agency, over 2,100 SARs have been reported by trained officers resulting in 167 referrals to the JTTF, 26 local terrorism cases opened, and 50 local arrests for other types of crimes.

The ISE-SAR Evaluation Environment provided a controlled environment to implement and assess standard processes for gathering, documenting, processing, analyzing, and sharing terrorism-related suspicious activity reports. It also produced enough results for the Federal Government to successfully evaluate the effectiveness of the NSI process on activities related to gathering, documenting, processing, and analyzing suspicious activities determined to be reasonably indicative of terrorism-related crimes. While the amount of information actually *shared* during the evaluation period was constrained by the limited number of participants and the timeframe involved, the Evaluation Environment demonstrated that the integrated NSI process works effectively and participating agencies experienced tangible benefits. This section highlights some important lessons-learned from the Evaluation Environment that contributed directly to the four key findings discussed above.

1. *Executive Leadership is Essential*

Evaluation Environment participants observed that executive sponsorship is critical to the successful adoption and implementation of a standard NSI process. For example, Chief Harold Hurtt of the Houston Police Department noted that "If you're not committed to it [the NSI] at the top of your organization, it's not going to happen. The officers may be introduced to it, but if there's not interest from the Chief or the person at the top of the organization, it won't be done properly."

Specific approaches for ensuring leadership commitment varied among participating agencies, but they all agreed on the need to articulate clear mission expectations and provide adequate training for conducting the SAR mission, including the need to safeguard privacy, civil rights, and civil liberties. Several participating sites elected to issue special or general orders signed by senior leadership during the course of the ISE-SAR Evaluation Environment, an approach that proved valuable in demonstrating top-level management commitment to the effort.

2. *NSI Implementation Must Leverage Existing Processes and Procedures*

Law enforcement agencies have been gathering and documenting SAR information for years. As a result, to meet the goal of establishing and implementing a standard nationwide SAR process, the ISE-SAR Evaluation Environment was able to effectively leverage existing processes and procedures already in place at participating localities. In most cases, participating sites were able to simply modify existing procedures to implement the standard NSI process. The ISE-SAR Functional Standard, for example,

does not prescribe the details of all processes, systems requirements, or other business rules governing the collection, processing, or sharing of SARs by law enforcement entities. Instead it provides a top-level process that builds on the well-established processes and business rules for suspicious activity reporting already in place at federal, state, local, and tribal agencies.

> *One large urban Police Department added a check-box to its existing field interview forms to specifically denote a report as a SAR. This allowed the form to be properly routed for processing and, more importantly, did not require the frontline officer to fill out a new form. The training of the officers on behaviors potentially indicative of terrorism-related criminal activity was the only new element in their process.*

By leveraging existing procedures and systems—building on the familiar—participating agencies were able to simplify the introduction of a new capability into their organizations, minimizing the impact on their processes and, most importantly, their people. Several sites have begun to institutionalize the use of SAR in their existing daily processes. One participating state fusion center has already incorporated the requirement to search both internal and external repositories of SAR information into its standard analytic process.

3. *Personal Relationships are Key When Introducing New Processes*

Despite the intent to minimize the burden on Evaluation Environment sites, even the best planned implementations of new processes requires sufficient time for personnel to become familiar enough with them to integrate them into their day-to-day activities. In the interim, personal relationships continue to be important for maintaining continuity of operations. In fact, a significant conclusion drawn from the ISE-SAR Evaluation Environment was that improved processes and technology enhanced effectiveness, but did not substitute for personal relationships in collaborating and sharing information.

The NSI cycle involves a series of routine steps that are fairly mechanical and which can be completed strictly internal to the participating agency. There are some steps, however, that depend on close collaboration among federal, state, local, and tribal agencies. During the Evaluation Environment, information sharing worked best when local site and federal personnel were either collocated or at least near one another.

Assignment of federal personnel to participating sites or rotation of state, local, and tribal personnel to operational units at the federal headquarters level enhanced collaboration and information sharing. Sites that maintained close relations with local federal analysts enjoyed greater access to information—both pushed and pulled—because local analysts were better able to convey to the federal partner a clearer understanding of the site's priorities and information needs. Federal analysts, working with fusion center personnel were better able to collaborate on work products, develop threat and risk assessments, and share information. Collocation of personnel also helped improve the quality and effectiveness of federal products developed to meet state, local, and tribal requirements.

4. *An Effective Training Program is a Critical Element of Success*

A well-developed and executed training program proved critical to the successful implementation of the SAR process. The NSI training program expands officers, investigators, and analysts' knowledge of behaviors and incidents indicative of terrorism-related criminal activity. This specialized training is important to the SAR process because, as noted in an important court case on this subject, conduct that may be innocuous when viewed in isolation can sometimes be determined to be suspicious when considered as part of the totality of the circumstances. [6] This guidance ensures that frontline law enforcement personnel, their supervisors, and the analysts who have responsibility for vetting SARs, have the proper context to make inferences about the cumulative information available to them, which enables them to carry out their responsibilities in accordance with laws, regulations, policies, and procedures that help safeguard privacy, civil rights, and civil liberties. [7]

> *At the beginning of the ISE-SAR Evaluation Environment, several participants reported holding between several hundred and several thousand legacy SARs considered to be potentially terrorism-related. Sites reviewed their holdings in accordance with terrorism behaviors as described in the ISE SAR Functional Standard and described in the Analyst Vetting course and, as a result, reprocessed the information, and significantly reduced the volume of data considered to have a potential nexus to terrorism. One site was able to filter out almost 95 percent of its reports by determining that they had no terrorism nexus. Analyst training helps preclude having "too many dots" to sort through by ensuring only those with relevant analytical value are shared. Training also enabled analysts to better understand the utility of accessing numerous public, private, federal, state, and local data repositories to gain valuable information and to enhance their performance.*

Accordingly, the NSI Project Team and its stakeholders—including BJA, FBI, DHS, IACP, MCCA, MCSA, and the National Sheriffs' Association—developed a specialized pilot training program specifically designed to address privacy, civil rights, and civil liberties safeguards. Members of the privacy, civil rights, and civil liberties advocacy community reviewed and provided valuable input to the three-part curriculum which included separate courses that provided specialized training targeted at three groups of people: executive-level personnel, frontline officers, and analysts.

---

6 See *United States v. Montero-Camargo*, 208 F.3d 1122, 1130 (9th Cir. 2000) (explaining that "sometimes conduct that may be entirely innocuous when viewed in isolation may properly be considered in arriving at a determination that reasonable suspicion exists").

7 See *United States v. Arvizu*, 534 U.S. 273 (2002) (explaining that the reasonable suspicion determination "allows officers to draw on their own experience and specialized training to make inferences about the cumulative information available to them").

The integrated training program was critical to establishing a standard NSI process. Significant results of the training included:

- A reduction in the number of SARs identified as potentially terrorism-related through better filtering;
- Improvement in the quality of SARs; and,
- An enhanced focus by all participants on ameliorating privacy, civil rights, and civil liberties.

As a result of the training program, frontline officers were better able to place observed or reported behaviors into context, maximizing their effectiveness in identifying potential criminal activity while minimizing the likelihood of documenting circumstances involving individuals engaged in innocent or constitutionally protected activities. Although there is insufficient data to draw definite conclusions, this suggests that training is improving the quality of reports from frontline officers and, consequently, making the analysts' jobs easier by providing them with higher quality inputs better conforming to the criteria in Part B of the ISE-SAR Functional Standard. More information is needed over the longer term to validate this observation.

5. *Threat Information and Tactical Risk Assessments Should Drive State and Local Information Needs*

A Congressional Research Service study on the NSI identifies a number of instances where police, acting in the normal course of their duties, arrested individuals who were acting suspiciously, and subsequently uncovered or disrupted terrorist plots.[8] An objective of the NSI process is that the discovery and disruption of these plots should not be merely a serendipitous result of unfocused information gathering but instead stem from an end-to-end process driven by clear information needs. Federal agencies must provide relevant threat information to state and local agencies that can contribute to local or regional threat and risk assessments and better inform local operational activity. To meet this objective, required steps include:

a. Identification and submittal of state and local information needs to appropriate agencies at the federal level;
b. Development of federal products in response to state and local information needs;
c. Completion of tactical risk assessments against potential threats; and

[8] Congressional Research Service Report R40901, "Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for congress, by Mark A. Randol (November 5, 2009).

d. Guidance to frontline officers on tactics, techniques and behaviors indicative of terrorism activities.[9]

During the course of the Evaluation Environment, DHS and FBI worked closely with participating agencies to define a process that would capture and respond to state, local, and tribal information needs. The NSI Concept of Operations, published after the Evaluation Environment was already underway, established an approach for sharing Terrorism Information Needs among federal agencies and state, local, and tribal organizations.[10] This process is still in its early stages, but once fully implemented, will assist in enabling more thorough and focused risk assessments by state, local, and tribal law enforcement in partnership with the Federal Government.

Based on an earlier case that the FBI solved in 2009, a major urban area fusion center refined the list of terrorism behaviors to watch for, updated training material, and briefed airport security personnel in the fusion center's area of responsibility. The result—attributable at least in part to better informed airport security personnel—has been more consistent and higher quality reports of relevant suspicious activity.

Tactical Risk Assessments are based in part on federal threat information about terrorist intentions, plans, and techniques. They add a local or regional dimension to that threat by examining the vulnerabilities of potential targets and assessing potential consequences should an attack be successful. Such assessments should result in improved information needs as well as better guidance to and more efficient use of public safety personnel to accomplish a more efficient allocation of limited resources. In addition, these assessments can contribute to frontline officer training by providing officers with the proper context within which to gather SAR information even where behavior may be seemingly innocent. For example, the act of photographing a bridge could take on more or less meaning and be met with a more informed and appropriate response when viewed in the context of current threat and risk assessments— the "totality of the circumstances" described in the earlier discussion on training.

Though not yet fully institutionalized, this front-end planning component of the NSI cycle has already demonstrated its value to the collection and reporting of information. During the course of the Evaluation Environment, state, local, and tribal agencies received Risk Assessment training using a case study based on the November 2008 terrorist attack in Mumbai where nearly 500 people were killed or injured. As a result of that training, a number of state, local, and tribal organizations are examining the risks to their critical infrastructure based on the terrorist tactics, techniques, and behaviors used in the attack.

9 *Nationwide Suspicious Activity Reporting Initiative Concept of Operations* (December 2008), pp 17-18. Available at http://www.ise.gov/pages/sar-initiative.aspx

10 Ibid. p. 23.

6. *Functional Standards Enable Effective Sharing of ISE-SARs*

The steps in the NSI cycle can be implemented in a number of ways, but the overarching process itself is what drives how technology is used as an enabling capability. The Evaluation Environment helped drive home the essential point that underlying functional and technical standards serve as important enablers for effective sharing.

Regardless of the particular implementation, the basis for sharing in the NSI is the ISE-SAR Functional Standard. This standard 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.[11] The standard provides the unifying glue that allows participating agencies with different technical implementations and systems to share information effectively and efficiently. It provides an important capability for representing details about terrorism-related suspicious activity in a standard format to help facilitate the identification of useful investigatory or trending information.

The NSI CONOPS describes a multilevel review process for identifying those SARs with a potential nexus to terrorism out of the thousands of suspicious activities documented by source agencies each day.[12] 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 and counterterrorism experts from across the country as being reasonably 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 pre-operational planning related to terrorism. If this determination is made, the report will be 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 consistent with the NSI Privacy Framework.

The major implementation approach used during the Evaluation Environment relied on a distributed environment consisting of multiple ISE Shared Space servers at participant locations. Information loaded into the ISE Shared Space servers can be searched, accessed, and displayed by all authorized ISE investigative and analytic personnel to support their counterterrorism missions. [13] Information remains under the local control of the participating agency. Another technical solution is the FBI eGuardian system, which is available for use by state, local, and tribal agencies. Information entered into

---

11 *ISE-SAR Functional Standard, Version 1.5* (May 2009) located at http://www.ise.gov/pages/sar-initiative.aspx

12 NSI CONOPS., pp. 7-11.

13 Ibid. Pp. 22-23.

eGuardian is to be replicated in a separate eGuardian shared space server and made available to authorized NSI participants. Although eGuardian is based on different technology and provides other capabilities, its ISE Shared Space server functions—for information sharing purposes—like all the others. The Department of Defense 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 are also already using or contemplating using eGuardian.

7. *Sharing Must be Accomplished in a Way that Protects Privacy, Civil Rights, and Civil Liberties*

Fundamental to the success of the NSI is the commitment to protect privacy, civil rights, and civil liberties guaranteed by the Constitution and laws of the United States. Prior to the start of the ISE-SAR Evaluation Environment, the PM-ISE and its federal partners analyzed potential privacy and civil liberties risks associated with ISE-SAR information sharing activities and consulted with privacy and civil liberties advocacy groups to identify effective mitigation tools. This process culminated in the issuance of an initial analysis which identified two key objectives:

a. Revision and adoption of the ISE-SAR Functional Standard; and
b. Development of a robust privacy protection framework. [14]

The Functional Standard, as revised in May 2009, identifies the types of activity that may be deemed suspicious and the circumstances under which such information may be shared.[15] By focusing on observed behavior, this standard mitigates the risk of profiling based on race, ethnicity, national origin, or religion. It also improves mission effectiveness by enabling agencies to scope and address potential threats in a more efficient and standardized manner.

The second key objective led directly to the development of what ultimately became the NSI Privacy, Civil Rights, and Civil Liberties Framework described more fully under Key Finding 2. Before a site may share or receive personal information contained in privacy fields, the site must ensure that its written policies and procedures satisfy applicable ISE Privacy Guideline requirements, including: (a) purpose specification; (b) notice mechanisms; (c) data quality; (d) data security; (e) accountability/enforcement and audit; and (f) redress.[16] The PM-ISE and its federal partners assisted the sites by developing privacy policy templates, offering technical assistance, and by reviewing each site's privacy policy. In addition, sites must ensure that all personnel are

[14] *Information Sharing Environment – Suspicious Activity Reporting Functional Standard and Evaluation Environment: Initial Privacy and Civil Liberties Analysis* (Sept. 2008) available at http://www.ise.gov/pages/sar-initiative.aspx

[15] *ISE-SAR Functional Standard, Version 1.5*, pp. 29-36.

[16] After a limited test to assess the value of ISE-SARs without privacy fields, it was determined that, at least for the EE, it was necessary to include privacy fields. As a result privacy policies and procedures were required to share any ISE-SARs.

adequately trained before the process begins (see Lesson-Learned 4 for a fuller discussion).

Revision of the Functional Standard and adoption of what became the NSI Privacy Framework effectively mitigated implementation risks during the ISE-SAR Evaluation Environment as the following results show:

a. No complaints for redress were filed;
b. No sites reported a breach of personal information contained in privacy fields;
c. After spending approximately six months developing and implementing their privacy policies, nine sites had privacy policies approved and in place
d. Privacy awareness was heightened as a result of extensive training of site personnel and by requiring personnel to review and certify acceptance of the site's privacy policy; and
e. The outreach efforts to the public and to privacy and civil liberty advocacy groups at the beginning of the ISE-SAR Evaluation Environment facilitated the identification and mitigation of potential implementation risks.

Such results show that the NSI Privacy Framework adds value and can be successfully implemented. In particular, the extensive training provided to key personnel heightened awareness of basic privacy safeguards. This heightened awareness, when implemented nationally, will form a solid foundation for achieving a consistent, appropriate response by law enforcement to suspicious activity within their jurisdiction.

The broader NSI implementation should address the following features as part of implementing the NSI Privacy Framework:

a. Sites must fully implement the Framework prior to participation in the NSI;
b. Participating agencies should continually assess and update their privacy policies and procedures and ensure they are fully integrated into business processes;
c. Sites should establish personal accountability for protecting privacy, civil rights, and civil liberties for all site personnel and participating agencies;
d. The NSI Program Management Office should continue to provide technical assistance to sites to support privacy policy adoption and implementation; and
e. Sites should have a trained privacy officer available to provide ongoing advice and assistance regarding privacy, civil rights, and civil liberties.

All NSI stakeholders are committed to a transparent NSI process to foster public trust. In early 2010, the ISE Privacy Guidelines Committee (Chaired jointly by senior privacy officials from the ODNI, DOJ, and DHS) will publicly release a final in-depth privacy analysis of the NSI Evaluation Environment that will describe lessons-learned in more detail and provide specific recommendations for moving forward with the nationwide implementation.

8. *Outreach and Collaboration with Community Leaders is Essential*

NSI success depends heavily on the ability to earn and maintain the public's trust. Although outreach and collaboration with community representatives at the local level was not an explicit requirement of the ISE-SAR Evaluation Environment at the outset, the *Building Communities of Trust* initiative was developed and piloted in four of the Evaluation Environment sites to help achieve greater collaboration and transparency. The initiative aims to develop relationships of trust between police, fusion centers, and the communities they serve, particularly immigrant and minority communities, so that the challenges of crime control and terrorism prevention can be confronted with the support of local communities.

The Building Communities of Trust initiative brought together police, fusion center, and community representatives in a roundtable setting to help build trust-based relationships and increase understanding of different concerns and perspectives. The groups discussed specific local concerns and reviewed how NSI implementation and training will help law enforcement determine the difference between innocent cultural behaviors and behavior indicative of criminal activity. Findings from the project will be available in early 2010 and are being incorporated into NSI nationwide implementation.

Recommendations

The following recommendations are designed to assist with NSI implementation; many are interrelated and will need to be addressed as part of NSI PMO planning.

1. *Establish a Program Management Office to Manage and Oversee NSI Implementation*

Based on recent White House direction, NSI implementation will enter a new, more formal phase starting in 2010.[17] In response, DOJ is establishing an interagency NSI Program Management Office (PMO) to manage implementation. PMO participation will include DHS, FBI, and other federal, state, local and tribal partners. The PMO, in conjunction with all NSI stakeholders, should ensure that the lessons-learned from the Evaluation Environment and recommendations in this report are incorporated into future implementation activities.

2. *Apply a Robust Framework to Protect Privacy, Civil Rights, and Civil Liberties*

Protection of privacy, civil rights and civil liberties is essential to the success of the NSI process. Accordingly, consistent with Key Finding 2, all agencies participating in the NSI must implement a Privacy Framework that includes the following elements: (a) demonstration that operations are conducted in accordance with laws, policies, and procedures consistent with the ISE Privacy Guidelines; (b) training of frontline officers, investigators, analysts, and supervisors on the behaviors and indicators of terrorism-related criminal activity; (c) a formalized, multi-layered vetting process for SAR and ISE-SAR information; and (d) a program of outreach and collaboration to the community, including privacy, civil rights, and civil liberties advocacy groups at the local level.

3. *Tailor Federal Information Products for Use by State, Local, and Tribal Agencies*

Although state, local, and tribal sites participating in the ISE-SAR Evaluation Environment found value in some of the threat assessments received from federal agencies, in many cases the information was too general to drive the Risk Assessment and Information Needs steps of the NSI cycle. The Interagency Threat Assessment and Coordination Group (ITACG), situated within the National Counterterrorism Center (NCTC), should continue to work closely with DHS and the FBI to ensure that federal information products are sufficiently specific to meet the needs of state, local, and tribal

[17] See http://www.prnewswire.com/news-releases/presidential-task-force-on-controlled-unclassified-information-releases-report-and-recommendations-79312237.html for additional information.

agencies. DHS and FBI, with ITACG participation, should also continue to work with state, local and tribal partners to ensure that the list of priority terrorism-related information needs is periodically refreshed.

4. *Institutionalize the NSI Risk Assessment Process*

An important step in the NSI cycle requires state and major urban area fusion centers, working with local representatives of federal agencies, to develop tactical risk assessments of potential terrorist targets within their jurisdictions. While there were some attempts to address this requirement as part of the Evaluation Environment, they were limited. The NSI PMO—working with DHS as it stands up a National Fusion Center Program Management Office—should coordinate with all relevant stakeholders to develop and test a standard methodology for completing tactical risk assessments and use the results to help develop information needs.

5. *Extend the NSI Process to an All Crimes Mission Environment*

The focus of the NSI to date has been specifically on SARs indicative of terrorism-related crimes (i.e., ISE SARs). However, almost all participating agencies operate in an "all crimes" environment where terrorism is only one of a number of criminal behaviors to which gathering and sharing of SARs is applicable. Consistent with Key Finding 4, the NSI PMO—working with DHS, FBI, and NSI participants—should lead an effort to incorporate an all-crimes approach into the NSI.

6. *Formalize NSI Feedback Mechanisms*

Feedback is an important part of the NSI cycle. During the ISE-SAR Evaluation Environment, feedback was provided largely on an ad hoc basis. The NSI PMO—working with DHS, DoD, FBI, and NSI participants—should ensure that standardized feedback mechanisms are adopted that, at a minimum, notify: (a) "source organizations" when information they provide is designated as an ISE-SAR by a "submitting organization" and made available for sharing; and (b) 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.

7. *Incorporate ISE-SARs into the Broader Analytic Process*

During the Evaluation Environment, the focus was on posting, viewing, and sharing SAR information. But as the national implementation gets underway, it is important to think more broadly about how SARs can and should be used as one important information source in a larger analytic process. DHS and the National Fusion Center PMO—working with the NSI PMO, DOJ, FBI, NCTC and the ITACG, PM-ISE, and other NSI participants—should develop analytic tradecraft and a methodology that will lead to the effective use of ISE-SAR information as a contributor to the larger counterterrorism analytic process. In addition, the NSI PMO—working with DHS, FBI, and the PM-ISE—should develop a methodology that supports the organization and display of SAR

information using analytic tools but still protects privacy, civil rights, and civil liberties and maintains control of the information by the submitting organization.

8. *Establish Training for Mid-level Managers*

Presentation of executive, frontline officer, and analyst training was fundamental to establishing the SAR process at participating sites and for ensuring the protection of privacy, civil rights, and civil liberties. However, as the evaluation progressed, it became increasingly apparent that mid-level managers, responsible for the daily direction and management of frontline officers, required equivalent training. The NSI PMO should ensure mid-level manager training is incorporated in future training plans and programs.

9. *Establish a Performance Measurement Plan for NSI Implementation*

A significant challenge faced by the PMO will be to establish effective performance criteria to measure the ultimate success of the NSI Program. Identifying appropriate metrics will be critical to determining outcomes. Performance plans should be reviewed to ensure they provide a results-oriented approach to monitor progress and performance, optimize resources, and promote accountability. While some output criteria may include data on the number of SARs produced and shared, the NSI PMO and all participating agencies should work to establish more mature indicators that support answers to target outcomes such as whether SARs produced and shared under the program are “meaningful,” and whether sharing achieves the objective of ensuring the “dots are connected.”

Appendix A - References

Available on PM-ISE Website (www.ise.gov)

Final Report on Presidential 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.

Final Report: Information Sharing Environment (ISE)-Suspicious Activity Reporting (SAR) Evaluation Environment, prepared by the Bureau of justice Assistance, (January 2010).

Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project (October 2008). A publication sponsored by BJA; MCCA; DOJ's Global Justice Information Sharing Initiative (Global), the CICC; DHS; and the FBI

ISE-SAR Evaluation Environment Segment Architecture (December 2008)

ISE-SAR Functional Standard, Version 1.5, ISE-FS-200 (May 21, 2009)

ISE-SAR Functional Standard and Evaluation Environment Privacy and Civil Liberties Analysis (September 5, 2008)

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing (October 2007)

Nationwide Suspicious Activity Reporting Initiative Concept of Operations (December 2008)

Others

Baseline Capabilities for State and Major Urban Area Fusions Centers: A Supplement to the Fusion Center Guidelines (September 2008) available at http://www.it.ojp.gov/default.aspx?area=globalJustice&page=1236

Fusion Center Guidelines: Law Enforcement Intelligence, Public Safety, and the Private Sector (October 2009), available at http://www.it.ojp.gov/default.aspx?area=globalJustice&page=1236

National Criminal Intelligence Sharing Plan, published in January 2006, serves as a foundation for a number of information sharing initiatives including the NSI. Available at http://www.it.ojp.gov/default.aspx?area=globalJustice&page=1236

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. Available at http://foia.fbi.gov/eguardian_threat.htm

Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress, Congressional Research Service Report (November 5, 2009), available at http://www.opencrs.com/

Appendix B - Acronyms and Abbreviations

BJA	Bureau of Justice Assistance
CICC	Criminal Intelligence Coordinating Council
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
FAMS	Federal Air Marshall Service
FBI	Federal Bureau of Investigation
IACP	International Association of Chiefs of Police
IEPD	Information Exchange Package Document
ISE	Information Sharing Environment
ISE-SAR	Suspicious Activity report determined to be reasonably indicative of terrorist-related criminal activity
ITACG	Interagency Threat Assessment and Coordination Group
JTTF	Joint Terrorism Task Force
MCCA	Major Cities Chiefs Association
MCSA	Major County Sheriffs' Association
NCTC	National Counterterrorism Center
NSI	Nationwide SAR Initiative
ODNI	Office of the Director of National Intelligence
PD	Police department
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager, Information Sharing Environment
SAR	Suspicious Activity Reporting

1

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