Nationwide SAR Initiative Annual Report 2010

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Table of Contents

Executive Summary

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office (PMO) initiated operations in March 2010 with the daunting challenge of ensuring that regardless of where in the country suspicious activity is reported, these potential indicators of terrorist activity can be analyzed and compared to other SAR information nationwide. This type of SAR analysis is at the heart of detecting and deterring a terrorist attack. Law enforcement agencies at all levels of government—state, local, tribal, territorial, and federal—have been collecting reports on suspicious activity, either from concerned citizens or businesses or through their regular duties, for years. The challenge for the NSI has been how to incorporate the informal processes that these agencies have historically used into the standards, policies, and processes developed by the NSI that allow analysts to compare and analyze SAR information from across the country and share this information with the critical law enforcement entities that need it to help prevent terrorist attacks.

Community and law enforcement outreach, standardized processes, training, a privacy framework, and enabling technology are the cornerstones for successful implementation of the NSI. Through strong leadership and outreach, the NSI works with key partners at the state, local, tribal, and federal levels of government, as well as advocacy groups, to not only develop the policies and processes of the NSI but also help ensure that Americans' privacy, civil rights, and civil liberties are protected throughout these processes. The NSI has done extensive outreach, engaging traditional and multidisciplinary law enforcement and homeland security partners to show transparency during the development and implementation of each of these important cornerstones.

The NSI's focus on these critical areas is paramount to the program's success. The program has made tremendous progress toward achieving nationwide integration, with 29 fusion centers serving as full partners within the NSI by March 2011 and the expectation of reaching every state and major urban area fusion center by the end of 2011.

In addition to law enforcement officers, the NSI is broadening its target audience to include critical infrastructure communities and public safety professionals—such as the fire service, emergency medical technicians, and the broader criminal justice field, such as probation, parole, and corrections partners. These communities are force multipliers to the existing SAR initiative. The NSI has made significant strides in its first 12 months of existence and is poised to expand its engagement in similar fashion with additional stakeholders.

Background

The findings in *The 9/11 Commission Report* and the Markle Foundation report[1] clearly demonstrated the need for a nationwide capacity to share information that could detect, prevent, or deter a terrorist attack. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 and the 2007 *National Strategy for Information Sharing* indicate both legislative and executive intent to establish locally controlled distributed information systems wherein potential terrorism-related information could be contributed by the 18,000 state, local, tribal, and territorial (SLTT) law enforcement agencies for analysis to determine whether there are emerging patterns or trends. Following this guidance, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) was born. The NSI is a partnership among federal, state, local, tribal, and territorial law enforcement that establishes a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information—also referred to as the SAR process—in a manner that rigorously protects the privacy and civil liberties of Americans. The ISE-SAR Functional Standard v.1.5 defines suspicious activity as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." This definition was developed after critical input from several privacy, civil rights, and civil liberties advocacy groups, including the American Civil Liberties Union (ACLU). The SAR process is critical to sharing information about suspicious activity with a potential nexus to terrorism, which can help prevent terrorist attacks and other related criminal activity from occurring. In developing the standards and processes, the NSI leveraged the guidance and expertise provided by the Global Justice Information Sharing Initiative (Global), which serves as a Federal Advisory Committee and advises the U.S. Attorney General on justice information sharing and integration initiatives. This includes leveraging the National Information Exchange Model (NIEM), which allows the interoperability and seamless exchange of information.

Support of the Nationwide SAR Initiative (NSI) efforts has been publicly stated by major law enforcement associations, including the International Association of Chiefs of Police (IACP), the Major Cities Chiefs Association (MCCA), the Major County Sheriffs' Association (MCSA) and the National Sheriffs' Association (NSA).

The NSI is a collaborative effort among SLTT and federal agencies, including the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice (DOJ); the Program Manager for the Information Sharing Environment (PM-ISE); the U.S. Department of Homeland Security (DHS); the Federal Bureau of Investigation (FBI); Global; and the Criminal Intelligence Coordinating Council (CICC).

On December 17, 2009, DOJ was named the Executive Agent to establish and operate the Program Management Office (PMO) for the NSI. Then in March 2010, DOJ established the PMO within BJA to support nationwide implementation of the SAR process. The PMO is responsible

[1] Markle Foundation Task Force Report, *Creating a Trusted Information Network for Homeland Security* (Markle Foundation, 2003)

for nationwide implementation of the SAR process by coordinating existing resources and managing additional support.

Implementation of the NSI

The NSI Program Management Office (NSI PMO) has established standardized processes and policies that provide the capability for SLTT and federal law enforcement to share timely, relevant SAR information that has been determined to have a potential nexus to terrorism, while working to ensure that privacy, civil rights, and civil liberties are protected. The national network of fusion centers is a critical part of this effort.

National Network of Fusion Centers

State and major urban area fusion centers (fusion centers) serve as primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among SLTT and federal partners. Located across the country, fusion centers are uniquely situated to empower frontline law enforcement, public safety, fire service, emergency response, public health, critical infrastructure/key resources (CIKR) owners and operators, and private sector security personnel to lawfully gather and share threat-related information. They provide interdisciplinary expertise and situational awareness to inform decision making at all levels of government. Fusion centers conduct analysis and facilitate information sharing, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.

The NSI PMO closely coordinates with the FBI and the DHS Office of Intelligence and Analysis (I&A) to ensure that technical, policy, and training requirements are met by fusion centers. As of March 2011, 29 fusion centers had implemented the NSI process and achieved operational status, with another 30 fusion centers in progress.

Tribal Outreach

The NSI PMO has been working to incorporate tribal law enforcement entities into NSI processes. In February 2011, the IACP Tribal Section agreed to endorse the NSI Line Officer Training, encouraging all tribal law enforcement members to train all officers on the behaviors that are potentially indicative of terrorist activity.

Private Sector and Critical Infrastructure/Key Resources

Protecting and ensuring the continuity of the critical infrastructure of the United States are essential to the nation’s security, public health and safety, economic vitality, and way of life. Critical infrastructure consists of the assets, systems, and networks so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. The NSI recognizes the importance of incorporating the private sector—which owns and operates more than 80 percent of the critical infrastructure and key resources in our country—and has therefore been working with the FBI and the DHS Office of Infrastructure Protection (DHS IP) to incorporate, over time, the 18 identified sectors within the *National Infrastructure Protection Plan* (NIPP) into the NSI process.

Sector-Specific SAR Reporting

In addition to the local and regional reporting and analysis of SAR information, critical infrastructure sectors—for example, chemical facilities, dams, transportation networks, and commercial facilities of all kinds—collaborate within their unique sector to identify trends, analyze sector-specific threats, and implement sector-wide protective measures.

In recognition of the sector-specific nature of critical infrastructure, the NSI supports the development of the *SAR for Critical Infrastructure* reporting tool. This tool is currently being piloted on the Homeland Security Information Network—Critical Sectors (HSIN-CS). Critical infrastructure owners and operators are able to share SAR information within their sector, allowing similar critical infrastructure facilities (other earthen embankment dams, specialty chemical plants, etc.) to gain awareness of suspicious activity occurring at like facilities. Suspicious activity reported to the HSIN-CS Web portal is immediately reviewed by the DHS National Infrastructure Coordinating Center (NICC), which is a 24/7 operations center and an operational element of the DHS National Operations Center (NOC). The NICC watch officers review SAR information against the Functional Standard to ensure that valid SAR information is entered into the NSI Federated Search via the DHS common box. The NICC also forwards SAR information to the FBI Counterterrorism Watch Unit (CT Watch), DHS I&A, and appropriate fusion centers. This tool and the associated processes are not intended to replace or discourage local suspicious activity reporting; rather, this is a supplementary tool to allow for data sharing within the sectors at a national level.

In relation, over the past year, Amtrak has been working with the NSI PMO to establish and integrate Amtrak's SAR capability with the NSI process. In establishing its SAR capability, Amtrak will utilize NSI's standardized processes, including training of analysts and frontline officers on protection of privacy, civil rights, and civil liberties and how to identify behaviors that may be associated with pre-incident terrorism planning.

Leadership and Interagency Support

The purpose of the PMO is to facilitate the implementation of the NSI across all levels of government and assist participating agencies in adopting compatible processes, policies, and standards that foster broader sharing of SAR information, while ensuring that privacy and civil liberties are protected in accordance with local, state, and federal laws and regulations. Primary functions of the PMO include advocating on behalf of the NSI, providing guidance to participants at all levels, and coordinating various efforts within the NSI. Given the criticality of privacy and civil liberties issues, the PMO works collaboratively with and is supported by the DHS and DOJ Privacy and Civil Liberties Offices, respectively.

NSI PMO Leadership

The Bureau of Justice Assistance, DOJ, was selected as the lead for the NSI and appointed both the Director and the Chief Technology Officer for the NSI PMO in February 2010, after having previously supported the development of SAR policy and processes. In March 2010, the DHS appointed a Principle Deputy Director, and the FBI appointed a Deputy Director to round out the executive leadership of the NSI, demonstrating the strong support for this interagency effort. Along with the executive leadership, DHS and the PM-ISE have also detailed senior executives to the NSI PMO to support nationwide training efforts, critical infrastructure and key resources outreach, and strategic policy development.

ISA IPC SAR Subcommittee

In December 2010, the Information Sharing and Access (ISA) Interagency Policy Committee (IPC) asked for the development of a SAR Subcommittee. The SAR Subcommittee is authorized by the ISA IPC, consistent with the IRTPA of 2004, as amended, and is responsible for policy assessment and recommendation; guiding development of strategy, guidance, and policy documents; resolving interagency issues; and ensuring interagency coordination on related efforts. This subcommittee is responsible for providing policy recommendations for gathering, analyzing, and sharing SAR information across levels of government, the private sector, and mission areas. The SAR Subcommittee's focus is on future high-level policies for federal SAR information sharing. Membership of the SAR Subcommittee is composed of those agencies that are members of the ISA IPC, and the subcommittee is chaired by BJA.

Privacy

The protection of privacy, civil rights, and civil liberties is paramount to the success of the NSI. Given this importance, the NSI has worked with key partners—including the ACLU and other advocacy groups—to develop protections that, when consolidated, make up the NSI Privacy Framework. The NSI requires each site to consider privacy throughout the SAR process by fully adopting the following NSI Privacy Framework prior to NSI participation:

Advocacy groups have served an essential role in the shaping of the NSI Privacy Framework, including participation in the Building Communities of Trust (BCOT) National Planning Team and development of the BCOT Guidance.

Privacy policy: It is a requirement of the NSI PMO that each participating agency adopt and implement a privacy policy that is at least as comprehensive as the ISE Privacy Guidelines and includes a SAR provision. Guidelines for these privacy policies are contained in the *ISE-SAR Privacy, Civil Rights, and Civil Liberties Protection Policy Template* or the *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*.[2] To help support this effort, DHS required that all fusion centers leveraging DHS Homeland Security Grant Program funds have protections in place that are determined to be at least as comprehensive as the ISE Privacy Guidelines within six months of their Fiscal Year (FY) 2010 grant award. In March 2011, fusion centers reached that milestone, and all operational centers had a privacy policy that was determined to be at least as comprehensive as the ISE Privacy Guidelines.

ISE-SAR Functional Standard: The current ISE-SAR Functional Standard reinforces constitutional standards, including the protection of rights guaranteed by the First Amendment and limitations on the use of certain factors—race, ethnicity, national origin, or religious affiliation—in the gathering, collecting, storing, and sharing of information about individuals. As a result of input from privacy advocates, the standard also includes reliability indicators. Through the use of Information Exchange Package Documentation (IEPD), the Functional Standard allows the originating agency to include or not include fields that contain personal information, based upon the agency's rules and policies.

Training: The message that protection of privacy, civil rights, and civil liberties is a vital part of the NSI process is communicated through each of the three trainings—chief executive, analyst, and line officer—and helps ensure that participants in the NSI adhere to these protections. In relation, the NSI strongly recommends that fusion centers and other NSI participants have access to the services of a trained privacy officer to provide ongoing advice and assistance regarding the protection of privacy, civil rights, and civil liberties. Please see the Training section of this document for more detailed information about current and future training programs.

In addition to the framework outlined above, the NSI business process includes privacy protections as information is reviewed and entered into the NSI Federated Search. This includes a vetting process prior to submitting the record, an audit trail that shows who has accessed the

[2] This document was developed to help fusion centers develop a comprehensive privacy policy and was provided to all NSI sites.

record, and purge/redress policies to ensure that information that is no longer relevant is pulled from the system.

Community Outreach and Awareness

Building Communities of Trust

While developing the business processes, standards, and privacy protections outlined above, the NSI recognized that as these new tools and business processes are adopted and implemented in local law enforcement agencies and fusion centers, it is important for local law enforcement to explain to their communities how these new tools will be used while ensuring the protection of citizens' privacy and civil liberties. The success of the NSI largely depends on the ability of law enforcement to earn and maintain the public's trust; therefore, NSI sites are encouraged to engage in outreach to members of the public, including privacy and civil liberties advocacy groups and private sector partners, in the course of privacy policy development and implementation. By fostering these relationships and building on the lessons of community policing, law enforcement agencies are able to learn more about the community, making it possible for officers and analysts to distinguish between innocent behaviors and behaviors that could be indicative of criminal activity. It is important for communities to know that their law enforcement agencies will work to protect the privacy, civil rights, and civil liberties of all citizens but that they also will help protect those who provide information from transgressions or revenge. A transparent process and collaboration with advocacy groups will also help reinforce the ongoing commitment to earn and maintain the public trust.

To date, BCOT Roundtables have been held in Boston, Chicago, Dearborn,* Austin, Las Vegas, Los Angeles, Miami, Minneapolis,* and Seattle.

*In partnership with DHS.

Therefore, the NSI, working with the DOJ Office of Community Oriented Policing Services (COPS), DHS, and the PM-ISE, collaborated to create the Building Communities of Trust (BCOT) initiative. This initiative focuses on developing trusted relationships among law enforcement, fusion centers, and the communities they serve and, in particular, focuses on the immigrant and minority communities, which have historically had distrusting relationships with law enforcement, to help these communities address their challenges of crime and terrorism prevention. This relationship between law enforcement and the community is important because information provided by community members may be that key piece of information that is needed to thwart a potential attack. Those people who live and work in the community are more likely to notice some type of change in behavior or activity—such as a change in work pattern or acquiring potentially hazardous materials—and are more likely to report this to their law enforcement agency if there is a positive, trustworthy relationship in which members of the community feel that officers will do what is right with the information provided to them.

To ensure that the voices of the community and local law enforcement were incorporated and to help with the planning of this initiative, a National Planning Team—composed of subjectmatter experts from state and local law enforcement; fusion centers; community and faith-based organizations; leadership from minority and immigrant communities; privacy and civil liberties advocates; and federal homeland security, justice, information sharing, and privacy and civil liberties officials—was brought together in May 2009 to shape the concept for the BCOT initiative.

Select sites that participated in the NSI Evaluation Environment volunteered to pilot the initiative and conducted a roundtable discussion with a diverse group of representatives from the local community, law enforcement, and fusion center leadership to explore how these groups can effectively engage in meaningful and ongoing dialogue to build relationships of trust. Each roundtable was planned for and developed by a local planning team and attended by representatives from the local community, the fusion center, local law enforcement, and local FBI and DHS representatives. From these roundtables, a guidance[3] document was developed for local police agencies, fusion centers, and communities that provides advice and recommendations on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities that appropriately distinguishes between innocent cultural behaviors and behavior that may legitimately reflect criminal enterprise or terrorism precursor activities. This document, released in October 2010, has been used as the foundation for roundtables held in Las Vegas, Chicago, and Los Angeles and will also be leveraged for roundtables that will be held in summer 2011.

In fall 2010, the NSI partnered with the DHS Office for Civil Rights and Civil Liberties in its countering violent extremism efforts by participating in roundtables in Minneapolis, Minnesota, and Dearborn, Michigan. Coordination of these efforts will continue throughout 2011 as DHS leverages lessons learned from BCOT to develop a countering violent extremism training curriculum for law enforcement.

[3] *Guidance for Building Communities of Trust* http://nsi.ncirc.gov/documents/e071021293_BuildingCommTrust_v2-August%2016.pdf

"If You See Something, Say Something™" Campaign

In July of 2010, DHS launched a national "If You See Something, Say Something™" campaign and announced a joint information sharing partnership with Amtrak as part of the NSI, highlighting the public's role in keeping our country safe and the Obama Administration's commitment to bolstering surface transportation security. The "If You See Something, Say Something™" campaign—originally implemented by New York City's Metropolitan Transportation Authority—is a simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime and to emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities.

The "If You See Something, Say Something™" campaign is being launched in conjunction with the rollout of the NSI. Both the "If You See Something, Say Something™" campaign and the NSI underscore the concept that homeland security begins with hometown security, in which an alert public plays a critical role in keeping our nation safe.

In March 2011, DHS Secretary Janet Napolitano announced the launch of the Department's new "If You See Something, Say Something™" public awareness video, available at http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm. The video demonstrates to the public some of the different types of suspicious behavior and activity they may see that should be reported to the proper authorities. The video has been made available to all fusion centers to use as a training resource and to support their public awareness outreach activities. For more information, please visit www.dhs.gov/IfYouSeeSomethingSaySomething.

FBI Outreach Programs

In an effort to reach out to the community and the private sector, the FBI has developed several outreach programs:

Domestic Security Alliance Council (DSAC)—The DSAC is a strategic partnership between the FBI and the U.S. private sector to enhance communications and promote the timely and effective exchange of information, which will advance the FBI mission in preventing, detecting, and investigating criminal acts, particularly those affecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets, and proprietary information.

InfraGard—This initiative supports an information sharing partnership between the private and public sectors for the purpose of protecting the nation's critical infrastructures (e.g., energy sources, transportation systems, and emergency services) against attack or failure caused by either foreign or domestic threats and to support all FBI investigative programs, including counterterrorism, counterintelligence, and criminal and cyber crime. InfraGard also supports the DHS mission to reduce and eliminate infrastructure vulnerabilities and to mitigate consequences.

Counterintelligence Division Domain Program—This program consists of the National Security Academic Alliance and the National Security Business Alliance. The Business Alliance exists to protect U.S. interests in the private sector from being targeted by Foreign Intelligence Services by developing partnerships at the corporate headquarters level, which will result in bidirectional sharing of actionable and relevant information. The Academic Alliance exists to provide a forum for the discussion of national security issues relating to academia, including to serve as a conduit for discussion between relevant federal agencies and the higher education community; to develop education efforts for higher education regarding better understanding of the missions and mandates relating to terrorism, counterintelligence, and homeland security; and to advise on a research agenda that can facilitate national security.

Training

The NSI training strategy is a multifaceted approach designed to increase the effectiveness of state, local, and tribal law enforcement professionals in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. The overarching goal of the training strategy is to facilitate agency implementation of the SAR process and to enhance a nationwide SAR capability. Over the past year, training has emerged as one of the top priorities of the NSI, with a focus on three broad areas of responsibility—chief executives, fusion center analysts (and designees), and frontline officers.

Frontline Officer Training—Frontline law enforcement personnel are trained to recognize those behaviors that have a potential nexus to terrorism. Their routine duties position them to observe and report suspicious behaviors or activities. The SAR Line Officer Training focuses on the critical role line officers have in the effective implementation of the SAR process by identifying and documenting suspicious activity. To efficiently deliver training to a large number of line officers in a timely manner, this training is delivered through a 15-minute CD that has been posted to several online/distance-learning formats.

Chief Executive Briefing—Law enforcement executives play a vital role in ensuring that the SAR process is not only successfully implemented but effectively supported. The SAR Executive Briefings focus on executive leadership, policy development, privacy and civil liberties protections, agency training, and community outreach. Fusion centers, law enforcement professional associations, and additional entities conduct these types of briefings in a variety of venues.

Line Officer Training—The NSI PMO, in coordination with the International Association of Chiefs of Police (IACP), the Major Cities Chiefs Association (MCCA), the Major County Sheriffs' Association (MCSA), and the National Sheriffs' Association (NSA), has been working to deliver the line officer training to all 800,000 sworn law enforcement officers. To date, 21,348 officers from all 50 states have received the training.

Chief Executive Briefing—As part of the kickoff to implementing NSI processes, a Chief Executive briefing is held to answer questions and inform chiefs on the NSI processes and policies. Briefings have also been provided to chiefs and executives within key law enforcement associations, such as the IACP Division of State and Provincial Police, MCCA, MCSA, NSA, the Association of State Criminal Investigative Agencies (ASCIA), and the American Probation and Parole Association (APPA).

Analyst Training—NSI PMO staff have trained 1,340 fusion center analysts in 50 states. These analysts represent 420 different federal, state, local, and tribal agencies.

Training the nation's 800,000-plus law enforcement officers has been and remains the key linchpin to enhance a nationwide SAR capability. To meet this challenge, a collaborative effort has been undertaken by the IACP's Division of State and Provincial Police, which represents 50 state police and highway patrol agencies; the Major Cities Chiefs Association, which represents 63 major cities; the Major County Sheriffs' Association, which represents counties or parishes with a population of 500,000 or more; and the full membership of the National Sheriffs' Association and the International Association of Chiefs of Police. The NSI has also coordinated delivery of this training with fusion center directors, as well as the Association of State Criminal Investigative Agencies.

These major law enforcement organizations have committed to train all law enforcement officers by autumn 2011, and the NSI PMO is working closely with these organizations, as well as others, to ensure nationwide rollout of this important training, which will help ensure that quality, relevant information is provided to trained fusion center analysts for vetting and analysis.

Analyst Training—Ensuring that SAR information is properly reviewed and vetted is critical to promoting the integrity of information submitted; protecting citizens' privacy, civil rights, and civil liberties; and successfully implementing the SAR process. The SAR Analytic Role Training focuses on the evaluation of SAR information to identify behaviors that may be associated with pre-incident terrorism planning and the process for sharing terrorism-related SAR information nationwide. Through this curriculum, analysts and investigators are trained to recognize terrorism-related pre-incident indicators and to validate—based on a combination of knowledge, experience, and available information—whether the behavior has a potential nexus to terrorism and meets criteria for submission. The training has been delivered in an eight-hour workshop format.

In March 2011, the NSI PMO released the document "Vetting ISE-SAR Data: A Pathway to Ensure Best Practices," which provides guidance for fusion center analysts when vetting SAR information, provides compliance with the ISE-SAR Functional Standard v.1.5, and outlines a step-by-step process to help analysts determine whether incoming SAR information meets the criteria to be considered an ISE-SAR and pushed to the NSI Federated Search.

The NSI PMO has been closely coordinating with the DHS SAR Initiative Management Group (DSI MG) of the State and Local Program Office within the DHS I&A. The DSI MG has the lead for providing SAR-related support to fusion centers and has also been tasked with providing NSI training and implementing NSI processes within all relevant DHS components. This continued relationship will be critical as the NSI completes initial implementation, provides access to the tools, and moves toward sustainment and utilization of these capabilities.

Training—Moving Forward

Development of separate but coordinated training efforts targeting traditional and multidisciplinary public safety professionals is a critical component of the success of the NSI.

Our nation's 2 to 3 million first responders, including 1.1 million firefighters, are uniquely able to complement what has previously been considered a law enforcement effort. Firefighters, emergency medical technicians, emergency managers, and other public safety officials are frequently called to noncriminal situations in which they may observe suspicious behavior. In addition, the nation's more than 2 million security officers can act as "force multipliers" to sworn law enforcement. These trained observers will receive further training on the SAR process, with a special emphasis on privacy and civil liberties.

The NSI PMO is committed to the development and delivery of a comprehensive set of SAR training programs to a wide array of audiences. To that end, this training is being developed to focus on the most basic of issues and questions confronting the effectiveness of state, local, and tribal law enforcement, public safety, justice, and critical infrastructure professionals in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism.

Public Safety/Justice—Public safety/justice professionals include those in the fire service, emergency medical services, emergency management, corrections, probation and parole officers, and 9-1-1 operators/dispatchers. The development of an online training course, using the SAR Line Officer Training as its foundation, is being assessed to provide public safety professionals with an overall awareness of the SAR process, emphasize the importance of privacy protections, and teach the most important signs of potential terrorist activities. Examples include noticing chemicals that are otherwise out of place for the environment, bomb-making materials, indicators of preoperational terrorist surveillance, and social engineering. The NSI PMO will work with public safety organizations and associations to ensure nationwide delivery of this training. This online training will leverage existing training programs frequently used by public safety professionals.

Critical Infrastructure—The private sector field includes the owners, operators, and protectors of the nation's critical infrastructure, including private security officers. Additionally, critical infrastructure partners are unique in that they are frequently the targets—not just potential observers—of terrorists. An online training, or independent study course, built upon the foundations of the SAR Line Officer Training will be developed and delivered to critical infrastructure security professionals nationwide. This planned course will be part of the training course for public safety officials and will again stress the components of the overall SAR process, privacy and civil liberties, and the most important signs of potential terrorist planning.

Next Steps

Discussions with public safety, justice, and critical infrastructure representatives will be held to determine the most useful training delivery methods and the most applicable course content. Discussions will focus on the applicability of the SAR data submitted and the role law enforcement officers play once they receive reports from these communities. The NSI PMO is planning to complete training content development by fall 2011 and will then explore the viability of wallet cards or pocket reference cards as possible easy-access, independently utilized training tools.

The NSI capitalizes on innovative technological solutions for information sharing by utilizing existing data collection methods and making them available through a federated search capability accessible to all the NSI partners.

Technology

Every day, in the course of their duties, law enforcement officers observe suspicious behaviors and receive such reports from concerned civilians, private security, and other government agencies. Until recently, this information was generally stored at the local agency and shared only within the agency as part of an incident reporting system. The Nationwide SAR Initiative (NSI) has taken the processes that law enforcement agencies have used for years and established a unified, standards-based approach for all levels of government to gather, document, process, analyze, and share information about behavior-based suspicious activities that potentially have a nexus to terrorism, while rigorously protecting the privacy, civil rights, and civil liberties of all Americans.

To support the operational mission, the NSI has leveraged the National Information Exchange Model (NIEM), which allows the interoperability and seamless exchange of information and was developed by the Global Justice Information Sharing Initiative (Global). NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner. NIEM standardizes content (actual data exchange standards), provides tools, and manages processes. By utilizing NIEM, the NSI has made it possible for agencies to search and share terrorism-related SARs across a federated environment.

How SARs Become Accessible Through the NSI Federated Search

There are two ways in which NSI participants can make their SARs available to the NSI Federated Search: by installing an NSI-provided server that leverages an existing legacy computer-aided dispatch (CAD) system or records management system (RMS) that is in line with NIEM standards or by creating an eGuardian account. NSI participants can access the NSI Federated Search through either RISSNET™ or Law Enforcement Online (LEO), and participants will be able to access the search through Homeland Security Information Network Law Enforcement (HSIN-LE) sometime in the future.

NSI Shared Space Server

The NSI-provided server—or common box—is a key element of the NSI Federated Search capability so SAR information can be accessed by fusion centers, DHS, and the FBI using legacy SAR systems and the FBI's eGuardian system, which allows the searching of SAR data nationwide and across state, local, tribal, territorial, and federal agencies. This process serves multiple purposes: (1) it normalizes local data so it can be searched not only by specific data elements but also by key word searches in the narratives, (2) it eliminates the need for officers and fusion center staff to reenter information, since it was already entered in their resident legacy system, (3) it precludes local agencies and/or fusion centers from having to change the way they currently collect SARs, and (4) it allows fusion centers to maintain local control of the SAR information while still sharing on a national level. The shared space server is a key element of the NSI Federated Search capability and is used not only by the fusion centers but also by the FBI's eGuardian and DHS to allow seamless searches of SAR data nationwide and across state, local, tribal, and federal agencies.

eGuardian

Deployed in 2008, eGuardian represents the FBI's participation in the NSI and the FBI's efforts to align with the Information Sharing Environment (ISE) mandate to establish a unified process for reporting, tracking, sharing, and assessing SAR information. The eGuardian system is a Web-based, cost-free tool accessed through the Law Enforcement Online (LEO) network that is secure but unclassified. It provides a platform for state and local police departments to share information with a potential nexus to terrorism among their own agencies and with fusion centers, other federal agencies, and the FBI. By utilizing the eGuardian system, the law enforcement community enjoys a previously unrealized degree of connectivity with regard to the collection and dissemination of suspicious activity and threat reporting, as well as a direct link to the Joint Terrorism Task Force (JTTF).

Prior to the rollout of eGuardian, the FBI concluded a Privacy Impact Assessment (PIA) on the eGuardian system. Pursuant to the eGuardian User Agreement and Rules of Behavior, users submit to mandatory privacy training to ensure protection of privacy and civil liberties.

The eGuardian system has more than 1,100 member agencies participating at the federal, state, and local levels, with more than 7,500 incidents entered into the system.

The U.S. Department of Defense (DoD) has just begun a multistage enrollment of users, which will result in the addition of approximately 8,500 users/contributors to the eGuardian system over the next year.

New Advances/Updates

As the number of fusion centers with access to the federated search tool increases, users have provided comments and recommendations on filtering methods that could assist with the search results returned by a user's inquiry. To address these needs, the NSI PMO has added two new features to the NSI Federated Search capabilities called "Map It/Link It." These new features enable users to enter specific search criteria, receive the listing of search results, and then click on the "Map It/Link It" tab to view the results geospatially, including the proximity of reported incidents. Also, a list of results will be generated down the side of the map that links specific SAR information with the search terms and will include the number of reports that meet the specific threat criteria. If the same person or vehicle is present in multiple SAR entries, it will be readily apparent and the user/analyst can quickly see whether there is a specific pattern or emerging trend. From this cursory review, an analyst would be able to look at the relevant SAR and potentially connect disparate incidents that may not be readily apparent. Also, this can help local law enforcement agencies support the deployment of resources to areas with higher levels of activity.

The NSI will also be adding a subscription feature in summer 2011 that will allow analysts to set search parameters and receive a notification when there is a report submitted that falls within these criteria.

ISE Annual Report

The ISE Annual Report to the Congress on the state of the Information Sharing Environment (ISE) is submitted in accordance with requirements in Section 1016(h) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, and Section 210D(c) of the Homeland Security Act of 2002, as amended. This report builds upon the mission partner accomplishments highlighted in the 2010 report and reflects:

- Progress on ISE implementation by the bureaus and agencies of federal, state, local, and tribal governments and private sector and international partners;
- Collective accomplishments of the terrorism and homeland security information sharing and access community;
- Individual agency initiatives that stand out as best practices in information sharing and help form the fabric of the ISE; and
- Successful partnerships between the PM-ISE and federal and nonfederal mission partners involving terrorism, homeland security, and weapons of mass destruction (WMD) information sharing.

The Program Manager, Information Sharing Environment (PM-ISE) facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices. Consistent with the direction and policies issued by the President and the Office of Management and Budget (OMB), the PM-ISE issues government-wide procedures, guidelines, instructions, and functional standards, as appropriate, for the management, development, and proper operation of the ISE. The ISE is realized by the investment of mission partners—the bureaus and agencies of federal, state, local, and tribal governments and our partners in the private sector and internationally—and is used by frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel.

The NSI is one of the ISE's most significant accomplishments to date and the best example of the ISE in action: an interrelated set of harmonized policies, mission processes, and systems that leverage ISE core capabilities and enablers to empower the men and women on the front line to access and share the information they need to keep the country safe. The 2010 ISE Annual Report highlights the many efforts of the NSI to help ensure the sharing of terrorism-related information among federal, state, local, tribal, and territorial law enforcement agencies, as well as the private sector.

Conclusion

As of March 2011, 29 of the 72 designated fusion centers have implemented the policies, processes, and standards that make up the NSI, with another 30 in progress and a goal of reaching all fusion centers by the end of 2011. This shows the advancements that the NSI has made toward ensuring that regardless of where in the country suspicious activity is reported, these potential indicators of terrorist activity can be analyzed and compared to other SAR information nationwide. The NSI has made tremendous progress toward achieving nationwide integration and continues to work with critical partners to help expedite this progress.

Besides law enforcement officers, the NSI is working to broaden its target audience to include multidisciplinary law enforcement partners, such as critical infrastructure communities and public safety professionals, firefighters, emergency medical technicians, and the broader criminal justice field. These communities are force multipliers to the existing SAR initiative and can play a critical role in supporting law enforcement agencies by sharing information that they come across in the course of their everyday activities and duties. The first 12 months of the NSI have been outstanding; the future successes are poised to be even greater.

Appendix 1—Resources

NSI Web site: http://nsi.ncirc.gov/

NSI Overview
Provides an overview of the Nationwide Suspicious Activity Reporting Initiative.

ISE-SAR Functional Standard
Builds upon, consolidates, and standardizes nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the processing, sharing, and use of suspicious activity information.

Privacy, Civil Rights, and Civil Liberties Protections: A Key Component of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)
Provides an overview of the privacy, civil rights, and civil liberties protections that serve as a foundational element of the NSI and are required in order to participate.

State and Local Anti-Terrorism Training (SLATT®) Program Terrorism Incident Database Overview
Provides an overview of the SLATT database, which allows users to track terrorism trends, identify areas of high activity, and match terrorism pre-incident indicators against similar cases, both past and present.

NSI Training Overview
Provides a description of the NSI training strategy and the three separate but coordinated training initiatives targeted towards law enforcement professionals with varying duties and responsibilities—agency executives, analytic/investigative personnel, and line officers.

Suspicious Activity Reporting Process Implementation Checklist
Provides a simplified checklist for chief executives and senior leadership to implement a SAR process within their agencies.

Final Report: Information Sharing Environment (ISE)—Suspicious Activity Reporting (SAR) Evaluation Environment
Provides lessons learned, best practices, and implementation steps identified during the ISE-SAR Evaluation Environment that can be utilized while implementing the NSI.

Policy Resources

Suspicious Activity Reporting Process Implementation Checklist
Provides a simplified checklist for chief executives and senior leadership to implement a SAR process within their agencies.

Nationwide Suspicious Activity Reporting Initiative Concept of Operations
Provides a common understanding of the NSI process so that implementation activities can be planned, executed, and measured.

Final Report: Information Sharing Environment (ISE)—Suspicious Activity Reporting (SAR) Evaluation Environment

Provides lessons learned, best practices, and implementation steps identified during the ISE-SAR Evaluation Environment that can be utilized while implementing the NSI.

Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project

This report and its recommendations are important for establishing national guidelines that will improve the identification and reporting of suspicious activity and will allow for the timely sharing of SAR information with law enforcement agencies, fusion centers, and the Joint Terrorism Task Forces (JTTFs).

National Strategy for Information Sharing

Sets forth a national plan to build upon progress and establish a more integrated information sharing capability.

Privacy Resources

Updated Privacy Policy Review Process

This document details the new privacy policy review process. It has been recently modified to support fusion centers and expedite the finalization of their privacy policies.

Fact Sheet: Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations Report for the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

This fact sheet provides a brief background on the NSI and a description of the privacy, civil rights, and civil liberties framework. It also lists highlights and observations and details recommendations for NSI implementation.

Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations: Nationwide Suspicious Activity Reporting Initiative

This report provides an update to the Initial Privacy and Civil Liberties Analysis published in September 2008. It contains a review of the development and implementation of the now concluded Information Sharing Environment Suspicious Activity Reporting (SAR) Evaluation Environment (EE) and makes recommendations to be followed during the nationwide implementation of the NSI.

Privacy, Civil Rights, and Civil Liberties Protections: A Key Component of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

Provides an overview of the privacy, civil rights, and civil liberties protections that serve as a foundational element of the NSI and are required in order to participate.

Technology Resources

ISE-SAR Functional Standard

Builds upon, consolidates, and standardizes nationwide aspects of those ISE-relevant activities already occurring at the federal, state, and local levels with respect to the processing, sharing, and use of suspicious activity information.

Enterprise Architecture Program

This document laid the foundation in defining practices and methodologies required to build implementable and executable information sharing enterprise architectures and to segment architectures leveraging core ISE principles.

eGuardian Privacy Impact Assessment

National Information Exchange Model (NIEM)

NIEM is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.

NSI Technology Fact Sheet

Provides an overview of the technology used within the NSI and includes technical diagrams for the ISE-SAR Shared Space.

Training Resources

Overview of Law Enforcement And Public Safety Channel (LEAPS.TV)

This document gives a brief overview of the Law Enforcement And Public Safety (LEAPS.TV) channel online, as well as instructions on how to access and view the SAR Line Officer Training CD through the LEAPS.TV Web site.

MIPT InCOP Overview

This document briefly describes the Memorial Institute for the Prevention of Terrorism's (MIPT) Information Collection on Patrol (InCOP^{SM}) workshop series. These workshops progressively enhance intelligence capability, both in traditional crime and terrorism prevention. InCOP 1, the first of the four courses, builds upon and reinforces the processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities, which is the core of the Nationwide Suspicious Activity Reporting Initiative.

FBI Virtual Academy

Other Resources

State and Local Anti-Terrorism Training (SLATT®) Program

The SLATT Program provides law enforcement personnel with specialized training and resources to combat terrorism and extremist criminal activity. A user name and password are required to access the SLATT Web site. To request a user name and password, please complete the Web site registration form.

2010 ISE Annual Report

ISE in the News

The Information Sharing Environment frequently posts articles about ISE Mission Partners. As a part of the ISE fabric, the NSI is often highlighted in these articles.

Appendix 2—Community Outreach Resources

Guidance for Building Communities of Trust

The Building Communities of Trust (BCOT) guidance provides advice and recommendations on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities that appropriately distinguish between innocent cultural behaviors and behavior that may legitimately reflect criminal enterprise or terrorism precursor activities. The guidance, available at http://nsi.ncirc.gov/itemsofinterest.aspx, was developed in partnership with select sites that participated in the Nationwide SAR Initiative (NSI) Evaluation Environment.

Communities Against Terrorism

Through the Communities Against Terrorism program, law enforcement agencies develop partnerships with their local business community to educate them on how to recognize terrorism/extremism warning signs and how to share the information with the right organization in order to prevent terrorism. To assist law enforcement agencies with their outreach efforts, various brochures are available for download on the SLATT Web site. To request a username and password for the SLATT Web site, please complete the Web site registration form.