



# NATIONWIDE SAR INITIATIVE

---

## ANNUAL REPORT 2011



This project was supported by 2011-DG-BX-K003 awarded by the Bureau of Justice, Office of Justice Programs, in collaboration with the Nationwide Suspicious Activity Reporting Initiative Program Management Office. 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 Briefing.....	1
Update on the Nationwide SAR Initiative .....	3
ISA IPC SAR Sub-Committee.....	5
Unified Message .....	6
Stakeholder and Community Engagement .....	8
Privacy .....	10
Training .....	11
U.S. Department of Homeland Security—SAR Analytics .....	15
Technology Improvements .....	16
Appendix 1—Resources .....	19
Appendix 2—Community Outreach Resources .....	24
Appendix 3—Unified Message.....	25

## Executive Briefing

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office (PMO) was established in March 2010 and is a collaborative effort led by the U.S. Department of Justice (DOJ), Bureau of Justice Assistance (BJA), in partnership with the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and state, local, tribal, and territorial (SLTT) law enforcement partners. The NSI PMO has been working with the National Network of Fusion Centers, hometown security partners, and SLTT and federal law enforcement to implement the policies, processes, and standards of the NSI across all levels of government while ensuring that privacy, civil rights, and civil liberties are protected.

Over the past year, the NSI PMO has brought in new staff members who have become essential in the continued development of the NSI. The addition of the Executive Support Specialists provides law enforcement and NSI experts to the field, so they can help NSI sites with training, technical assistance, policy development and guidance, and outreach to key stakeholders and chief executives, while also ensuring that NSI sites have met all of the requirements for implementation. The NSI has worked diligently in implementing the standards, policies, and processes of the NSI across the National Network of Fusion Centers, and as of March 2012, 68 fusion centers have the capability to contribute and share suspicious activity reports, expanding the reach of the NSI to over 14,000 law enforcement agencies in 46 states, including the District of Columbia. The expansion of the NSI has allowed the Federated Search Tool to be accessed by more trained users—increasing the number of searches to more than 43,000—and over 17,000 SARs were submitted for sharing by the end of March 2011.

Since the inception of the NSI, the FBI has been a vital partner in the success of sharing terrorism-related information. Over the past year, the FBI's eGuardian team has worked closely with the NSI PMO to address and finalize issues with system compatibility, data synchronization, and alignment of policies. Through their commitment to work together, the NSI PMO and the FBI conducted outreach to the National Network of Fusion Centers to ensure that NSI sites understand the SAR reporting process, as well as the full integration of the eGuardian system and how this will help continue to improve the sharing of suspicious activity.

Launched in conjunction with the NSI, the DHS "If You See Something, Say Something™" campaign made major strides over the past year in raising public awareness of indicators related to terrorism and encouraging individuals to report suspicious activity to their local law enforcement authorities. Also, to help support the efforts of the NSI PMO, the DHS Office of Intelligence and Analysis began working to establish baseline metrics and to evaluate the analytic value of SAR information submitted to the NSI Federated Search. This will help provide support for requests for information across the divisions, as well as external state and local support requests (SLSRs), NSI-derived production of Roll Call Releases, and support to other products.

The NSI PMO has maintained a focus on reaching out to key stakeholders across the country, informing them of updates and advances to current NSI programs and training initiatives, as well as technology

improvements. In the past year, the NSI Line Officer Training has been delivered to agencies and associations all over the country, and with their effort, approximately 250,000 frontline officers have reported receiving the training. With the success of the NSI Line Officer Training, the next task the NSI took on was to produce a SAR awareness training program for partners with similar missions to those of law enforcement constituencies, also referred to as hometown security partners, on behaviors and indicators of terrorist-related activity that they may come across while performing their daily responsibilities. The NSI PMO, with the assistance of subject-matter experts, developed sector-specific training for fire service and emergency medical services personnel, public safety telecommunications professionals (e.g., 9-1-1 operators), emergency managers, corrections and probation and parole officers, and private sector security personnel and those charged with protecting the nation's critical infrastructure.

Along with the development of the SAR Hometown Security Partners Training, the NSI PMO has continued to work with local law enforcement agencies on building relationships with community leaders through the Building Communities of Trust (BCOT) initiative. This initiative focuses on developing trust among law enforcement, fusion centers, and the communities they serve, particularly immigrant and minority communities, so that crime and terrorism can be addressed. The newly published *Building Communities of Trust: A Guidance for Community Leaders* was developed in partnership with DOJ, DHS, and the International Association of Chiefs of Police (IACP) to assist community leaders in working with law enforcement agencies to facilitate dialogue and discuss ways to work together to prevent crime and terrorism.

In addition to outreach to stakeholders and the community, over the past year the NSI PMO worked with the Office of the Program Manager, Information Sharing Environment (PM-ISE); the FBI; IACP—specifically the IACP Homeland Security and Terrorism Committees—and many other key federal, state, and local representatives and law enforcement associations to develop a Unified Message that reinforces the importance of SLTT and federal entities working together to fight terrorism and help keep our communities safe. This document reiterates the importance of suspicious activity reporting and training frontline law enforcement officers so they know what behaviors and indicators to look for while still ensuring privacy, civil rights, and civil liberties protections when they do. This message also underscores the importance of the sharing of SAR information with the FBI's Joint Terrorism Task Forces (JTTFs) for further investigation and with state and major urban area fusion centers (fusion centers) for analysis. The Unified Message also reinforces the important role local communities play and encourages them to work together with DHS on the "If You See Something, Say Something™" campaign, which raises public awareness of behavioral indicators of terrorism and emphasizes the importance of the public in reporting suspicious activities to local law enforcement.

Over the past year, the NSI PMO made a number of technology improvements to the NSI Federated Search and has also provided resources to assist users, if needed. These new modifications include a Single Line Search, similar to a Google search; a subscription service, where users can create and save queries; a new NSI Analytical Tool that will allow users to review specific information easily; and also a Help Desk and Frequently Asked Questions (FAQs) site, where users will find useful information pertaining to the NSI program.

## Update on the Nationwide SAR Initiative

### NSI Program Management Office (PMO)

The NSI PMO welcomed aboard new staff members during the past year: in March 2011, the FBI detailed a new Deputy Director, and in November 2011, the DHS detailed a new Principal Deputy Director. The NSI PMO also welcomed four Executive Support Specialists to the team this year. This team of highly qualified state and local law enforcement leaders is charged with providing hands-on technical assistance to NSI sites within their specific region and ensuring that those sites have met all of the requirements for NSI implementation. This includes scheduling needed training; providing executive briefings, policy development, and guidance; and educating sites on technical updates to the Federated Search. In addition, the Executive Support Specialists are able to help sites strategize on deployment of the frontline officer training, which is a critical component of the NSI process.

### Implementation

The NSI PMO staff worked diligently over the past 12 months to implement the standards, policies, and processes of the NSI across the National Network of Fusion Centers. As of March 2012, 68 fusion centers had the capability to contribute and share suspicious activity reports, as well as DHS, the FBI, and Amtrak. Outreach efforts are under way to implement the final participating fusion centers, which include fusion centers that were just stood up in 2011, into the NSI process. The expected completion of this is September 2012.

The NSI, through the National Network of Fusion Centers, now reaches over 14,000 law enforcement agencies in 46 states and the District of Columbia.

### Utilization

As the NSI has expanded to more sites, there has been a commensurate increase in users and utilization of the NSI Federated Search. As of March 2012, more than 43,000 searches had been conducted and over 17,000 SAR reports were available for analysts to search in the system. Maturity of the NSI has served as a strong enabler for fusion centers in developing relevant products that advance the situational awareness of their mutual stakeholders. Fusion centers are uniquely situated to provide an analytic context to SAR data, an essential element of the NSI's overall mission.

### Incorporation of eGuardian

eGuardian has been a partner with the NSI ever since the NSI's official inception in 2010. As such, the FBI has worked continually with the NSI in order to ensure that eGuardian and the NSI's Federated Search complement each other to achieve a shared mission of preventing terrorism by effectively sharing SAR data. Continued improvements over the past year have addressed system compatibility, record retention policies, data collection synchronization, and unified outreach to fusion centers regarding SAR reporting. The FBI's classified Guardian system (to which eGuardian migrates suspicious activity reports for investigative follow-up) has administered record retention policies that closely mirror

those of 28 CFR Part 23, the federal regulation that governs how law enforcement agencies operate criminal intelligence information systems while properly protecting individuals' privacy, civil rights, and civil liberties. In addition, the NSI has taken steps to facilitate the automated migration of SAR entries from the Federated Search to eGuardian in order to ensure that they are received by a JTTF. The FBI, the NSI, and DHS have also worked to foster a unified approach towards educating fusion centers on the changes that have taken place with respect to the SAR reporting process. Through a commitment by both the FBI and the NSI to ensure the integration of eGuardian and the Federated Search, similar improvements and enhancements will continue to be implemented to ensure the seamless sharing of terrorism-related information. The value of JTTFs in receiving SAR data is exemplified by the fact that over 700 terrorism investigations have been initiated by the FBI based on information received from eGuardian (April 2012).

An eGuardian incident was entered by FBI Headquarters (FBI HQ) personnel after an Internet tip from the Philippines claiming a named crew member of a privately owned cruise ship was intentionally infecting Americans with the AIDS virus. The subject was also about to place an explosive device on the ship with the intention of killing Americans. FBI HQ personnel were able to determine that the corporate headquarters for the cruise line was in Seattle, Washington. The incident was being prepared for transfer within the Guardian system to the Seattle Division. The legitimacy of the information was not known, nor was the name or whereabouts of the ship to which the subject crew member was supposedly assigned. Within minutes after placing the unclassified information into eGuardian, a telephone call came to FBI HQ from an analyst at the Pacific Regional Information Clearinghouse (PacClear). The analyst had an eGuardian account and noticed this new incident, which listed the contact number for the person who created it. The analyst was able to verify that a person with the same name as the subject had entered the United States from the Philippines on an employment visa and was in fact an employee of the named cruise line. Further, the analyst advised that the subject was assigned to a ship that was currently docked in Miami. This example of information sharing allowed FBI HQ to immediately forward the time-sensitive incident, via Guardian, to the Miami JTTF instead of the Seattle JTTF. The Miami JTTF was able to quickly locate both the ship and the subject. It was determined that the subject had sent e-mails indicating an intention to carry out a terrorist act; however, no explosives were found, and the pending threat was immediately mitigated. The collaboration between eGuardian and Guardian and between the fusion center and the FBI JTTF allowed for a quick response by law enforcement. Had this been a legitimate threat, this act of terrorism would have been prevented.

## **Expanded Efforts**

### Gang Data Exchange Standard Pilot Implementation

This initiative builds on the work of the Global Justice Information Sharing Initiative's (Global) Intelligence Working Group's (GIWG) Gang Intelligence Strategy Committee (GISC) and the Criminal Intelligence Coordinating Council's (CICC) efforts to improve and enhance national capabilities to share gang data. The first step completed was the development of the Gang Information Exchange Packet Document (IEPD), which identifies the data elements to be shared in a national Federated Search, as well as to identify statewide gang initiatives for use in a pilot project. The goal of the project is to have the National Gang Federated Search Tool located on the National Gang Intelligence Center (NGIC) Web

site, within a secure environment, which will be accessible through both the FBI's Law Enforcement Online (LEO) and the Regional Information Sharing Systems® (RISS).

Another aspect of the project is to look at the gang data elements in the FBI's Violent Gang and Terrorist Organization File (VGTOF) and determine whether it is possible to conduct an electronic push of data from local gang systems in the future. The project will also look at utilizing VGTOF as a data source in the Federated Search.

This initiative was developed based on the lessons learned of the NSI, including the segment and solution architecture and the technological relationship with fusion centers, as well as how to facilitate the sharing of information in a secure manner while providing an economic solution that maintains local control.

#### Terrorist Screening Center

The Terrorist Screening Center (TSC) is the agency responsible for maintaining the U.S. government's consolidated Terrorist Watchlist, which is a single database of identifying information about people who are known or reasonably suspected of being involved in terrorist activity. Over the past several months, the TSC and the NSI PMO entered into discussions about providing an electronic notification to the fusion centers and notifying multiple fusion centers as needed. The TSC is currently working to develop an electronic bulletin board on a secure but unclassified (SBU) system to post timely TSC encounter information and is also developing an immediate notification mechanism that simultaneously sends e-mail alerts to fusion centers.

### **ISA IPC SAR Sub-Committee**

The Information Sharing and Access (ISA) Interagency Policy Committee (IPC) Suspicious Activity Reporting (SAR) Sub-Committee is a results-oriented body responsible for providing the ISA IPC policy recommendations for gathering, analyzing, and sharing SAR information across levels of government, the private sector, and mission areas. The SAR Sub-Committee's focus is on broader policies for SAR information sharing, as opposed to the NSI, which is focused on implementation of the standardized process for gathering, analyzing, and sharing terrorism-related SAR information.

In 2011, the SAR Sub-Committee met six times, focusing on expanding support to SAR at the federal level through policy and guidance, as well as recommending priorities for evolution of the NSI. This included the development of best practices for analysts in the field to fully utilize SAR information, developing a Concept of Operations for SAR analysis at the federal level, and determining next steps for using the NSI model for a larger priority crimes platform.

## Unified Message

The attacks of 9/11 and the current dynamic threat environment demonstrate that no single organization can address terrorism alone. Every agency connected to the NSI mission, from the federal government to local police and sheriff's departments, must work together to share information that may prevent the next attack. Until recently, the federal government did not always provide clear, consistent guidance to SLTT and private sector partners on how and where to share information relating to suspicious activity. To help clarify the message and enhance existing partnerships and information sharing, the IACP hosted a series of meetings with very senior representatives from state, local, and

**Efforts to address crime and threats in our communities are most effective when they involve strong collaboration between law enforcement and the communities and citizens they serve. Law enforcement and homeland security professionals are responsible for ensuring that the public understands how to report suspicious activity and that agency/organizational members support the collection, analysis, and submission of suspicious activity reports to the proper fusion center or FBI JTTF.**

federal agencies, as well as law enforcement associations and other stakeholders, to create a unified approach to the reporting and sharing of information related to suspicious activity.

As a result of these meetings and coordination, there is now broad consensus on the message among law enforcement, homeland security agencies, and associations. A Unified Message document was created that provides clear guidance to the public that they should report any suspicious activity to law enforcement. The

Unified Message encourages agencies at all levels—state, local, tribal, and territorial—to work with DHS on its “If You See Something, Say Something™” campaign to raise public awareness of behavioral indicators of terrorism and to emphasize the importance of the public in reporting suspicious activities to the proper law enforcement authorities, who will forward suspicious activity reports to the FBI’s JTTFs for further investigation and to fusion centers for analysis.

The Unified Message also reinforces the importance of frontline officer training on identifying and reporting those behaviors and activities that are potentially indicative of terrorist or other criminal activity and provides direction to agencies on preparing SARs and how to ensure the protection of privacy, civil rights, and civil liberties when doing so. The Unified Message calls on law enforcement executives to conduct SAR training within their agencies and provides online resources for their use. The NSI PMO and the FBI worked closely together to ensure the interoperability between two systems: eGuardian and the Shared Space. Whether personnel enter a SAR into the eGuardian system or the Shared Space system, the other system will receive it.

The constantly evolving national security threat requires an adaptable information sharing strategy. The NSI PMO is committed to the timely sharing of intelligence and will continue to work with federal, SLTT, and private sector partners to implement and mature the NSI.

The complete document, *A Call to Action: A Unified Message Regarding the Need to Support Suspicious Activity Reporting and Training*, is located in Appendix 3.

On July 12, 2011, at approximately 17:00 hours, two U.S. military personnel, one in U.S. Marine Corps (USMC) uniform and the other in civilian attire, were traveling northbound on Interstate 5 in Seattle, Washington, in a government-licensed vehicle after leaving the Seattle Military Entrance Processing Station (MEPS). A blue Geo Metro vehicle, with Washington plates pulled up beside them and then braked in order to get behind them. The male driver of the Geo Metro (later identified as Mr. Michael McCright) appeared to look at the government license plate, then sped up to pull abreast of their vehicle. After a few seconds, Mr. McCright suddenly swerved his vehicle at the government vehicle in an attempt to run it off the freeway. The Marines pulled off the freeway and called 9-1-1 to report the incident.

After returning to the Marine Corps Recruitment Office, the Marines also reported the incident to their Commanding Officer. The information was then passed to the Antiterrorism (AT) Officer for the 12th Marine Recruiting District, in San Diego, California. The AT Officer then initiated a Tip and Lead (T&L) report, which was ultimately forwarded to the Washington State Fusion Center (WSFC) as a result of the officer's past interactions with a fusion center in California. Once the T&L arrived in the WSFC's Intake e-mail, it was reviewed by an intake analyst for processing. The intake process identified inconsistencies in Mr. McCright's activities and necessitated further vetting and investigation of the situation with more thorough background checks and case preparation. Simultaneously, a suspicious activity report (SAR) was entered into the Nationwide SAR Initiative (NSI) database, and the case was assigned to a fusion center detective for investigative follow-up.

A Washington State Patrol (WSP) detective currently assigned to the WSFC coordinated the case with the Seattle Division Joint Terrorism Task Force, which corresponded with an existing FBI investigation. The joint investigation quickly unveiled the severity of Mr. McCright's motives when it was discovered that he had recently been in cell phone contact with Mr. Abu Khalid Abdul-Latif, who was charged in the recently foiled Seattle terrorism plot in June 2011. Mr. Abdul-Latif, of Seattle, and Mr. Walli Mujahidh, of Los Angeles, California, were charged with plotting to attack the Seattle MEPS with small-arms fire and grenades. Contact or communication with known or suspected terrorists is viewed by the Intelligence Community as an observable violent or criminal radicalization behavior. Based on the investigation, an arrest warrant was obtained. Mr. McCright was arrested on September 8, 2011, on two counts of assault in the second degree. The arrest was conducted to ensure that Mr. McCright would be in custody prior to the weekend of the ten-year anniversary of the September 11, 2001, attacks, and because of his ties to a known terror suspect, his bail was set for \$2 million. Further investigation was conducted regarding his possible ties to other violent extremists and possible involvement in suspicious surveillance of a military recruiting center.

The process—from reporting the suspicious activity to the investigation and through to the arrest—was successful due to the emphasis placed on reporting suspicious activities to the appropriate law enforcement authorities and the deep collaboration among the WSP, the Seattle Police Department, the FBI, and the WSFC.

## Stakeholder and Community Engagement

### Speaking Engagements

The NSI PMO has made it a priority to reach out to key stakeholders, informing them of current activities as well as future plans and developments within the NSI program. Over the past year, NSI PMO representatives participated in more than 80 conferences and executive-level meetings, cutting across law enforcement; private industry; emergency management; fire and EMS services; corrections, probation, and parole; and critical infrastructure and key resources sectors. This outreach has helped inform the development of training and has been critical to ensuring that stakeholders understand the standards, policies, and processes of the NSI as they are being implemented and as the program matures beyond providing the capabilities and into the utilization of those capabilities by those in the field.

### NSI User/Analyst Meetings

In February 2011, the NSI PMO began hosting semiannual invitation-only Analyst User Meetings. These meetings are designed to highlight technological/system enhancements, engage in candid discussion on the use of the NSI Federated Search and eGuardian, identify SAR analysis best practices, resolve common debates regarding the vetting process, and make suggestions for additional training for analysts. Two of these meetings were held in the past year, and fusion centers were asked to identify analysts or other personnel from their fusion center who are the most familiar with vetting and analysis of SAR data and routinely utilize the NSI Federated Search. These regular, in-person feedback sessions are designed to improve the processes of the NSI and ensure that the technical functions of the Federated Search meet the needs of the field, as well as help shape future select policy issues as the NSI matures.

### ***Building Communities of Trust: A Guidance for Community Leaders and Program Update***

The Building Communities of Trust (BCOT) initiative focuses on developing trust among law enforcement, fusion centers, and the communities they serve, particularly immigrant and minority communities, so that crime and terrorism can be addressed. This initiative has been administered primarily by the NSI, a program that provides law enforcement with a capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity reports about behaviors that have a potential nexus to terrorism. The NSI recognizes that each community has one of the most important roles in the prevention of crime and terrorism, since law enforcement agencies are dependent on community members to report suspicious activity information to SLTT law enforcement officers. To help ensure that this reporting takes place, it is essential that law enforcement and community members have strong, trusting relationships. As these relationships are developed and maintained, members of the community are more likely to report crime and suspicious activities, which is why the NSI has worked with partners at the federal, state, and local levels—including U.S. Attorneys' Offices, privacy advocacy groups, faith leaders, and a diverse group of local community members—to implement the BCOT initiative.

Over the past year, the NSI, in coordination with DHS and the IACP, worked with local law enforcement agencies across the country to host Building Communities of Trust roundtables. The purpose of these meetings was to help open dialogue between law enforcement and community leaders, as well as to inform about the development of a new product, [\*Building Communities of Trust: A Guidance for Community Leaders\*](#). This document provides recommendations, resources, and tips on proactively working with law enforcement agencies to keep neighborhoods safe.

The BCOT initiative was also highlighted as a best practice in the White House Strategy “Empowering Local Partners to Prevent Violent Extremism in the United States” and subsequent Strategic Implementation Plan. The BCOT initiative was also featured in the Countering Violent Extremism (CVE) Workshop sponsored by DHS in Columbus, Ohio, in August 2011.

BCOT partnered with the IACP and DHS this year by holding meetings in several major urban areas, including San Francisco, California; San Jose, California; Oakland, California; and Aurora, Colorado. Because of the previous successes with roundtables held in 2010, follow-up sessions were also held in Chicago, Illinois, and Seattle, Washington, at the request of the law enforcement agencies and in coordination with the local U.S. Attorneys’ Offices.

#### **“If You See Something, Say Something™”**

The DHS “If You See Something, Say Something™” campaign, a public awareness and engagement initiative encouraging public reporting of suspicious activity to local law enforcement, has continued to grow since its initial launch in July 2010.

The campaign was originally used by New York’s Metropolitan Transportation Authority (MTA), which licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime-related efforts. The “If You See Something, Say Something™” campaign is being launched in conjunction with the rollout of the NSI. A critical element of the DHS mission is ensuring that the civil rights and civil liberties of persons are not diminished by our security efforts, activities, and programs. The “If You See Something, Say Something™” campaign focuses on behaviors and indicators, rather than appearance, in identifying suspicious activity.

Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious. For that reason, the public should report only suspicious behavior and activities (e.g., an unattended backpack in a public place or someone trying to break into a restricted area) rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity. Only reports that document behavior reasonably indicative of criminal activity related to terrorism will be shared with federal partners.

Partnerships include a variety of cities and states, universities, private companies, and all of the major sports leagues, including Major League Baseball, Major League Soccer, the National Basketball Association, the National Football League, the National Hockey League, the U.S. Open—Golf and Tennis, and IndyCar and NASCAR, as well as Minor League Baseball. DHS will continue to work to expand the initiative in the coming months.

A California motorist noticed a very muddy vehicle traveling on a highway near Los Angeles. As the motorist passed the vehicle, he noticed two occupants—a male driver and a female passenger—who were videotaping themselves. The female passenger appeared to be holding a device with wires coming out of it. When the driver in the muddy vehicle became aware that the other motorist had noticed them, he pulled a mask down over his face and sped away. The motorist was able to obtain the vehicle registration plate and reported the incident to local police, who checked the residence of the registered owner but were unable to locate him or the vehicle. The report was also placed into eGuardian by the local police agency. The local JTFF immediately received the incident after the transfer from eGuardian to Guardian and began checking internal FBI databases, as well as other publicly available sources. The JTFF determined that a telephone number of the suspicious vehicle owner had been in contact with a telephone number belonging to other persons under indictment in Washington State for terrorist acts, including a plot to kill U.S. government employees and police officers. Had this information not been effectively shared with the FBI, where internal systems could be cross-referenced, the associated telephone numbers would likely have never been discovered. As a result of this suspicious information, which was provided by a local police agency utilizing eGuardian, nefarious associations were found and a new terrorism investigation was initiated.

### **International Association of Chiefs of Police Information Sharing 101 Training**

The continued partnership of the NSI PMO with the IACP was strengthened over the past year with the inclusion of SAR principles and practices within the recently released curriculum supporting the State, Local, and Tribal (SLT) Domestic Security project, also known as SLT101. Through this project, the IACP has developed a curriculum designed specifically to address the growing demands of SLT agencies to better participate in the Information Sharing Environment (ISE). This training includes a seminar and online tutorials and will provide attendees with a resource tool kit to help guide the process.

The purpose of this training is to increase the knowledge of law enforcement executives of the various aspects of the ISE and to close the information gaps that may exist. Additionally, this training is designed to promote information sharing and analysis for the purpose of safeguarding communities in the United States while protecting the privacy, civil rights, and civil liberties of citizens. Special emphasis was given to the NSI, implementation of Fusion Liaison Officer (FLO) or Terrorism Liaison Officer (TLO) programs, and increased interaction and connectivity with fusion centers.

This training was held in ten locations across the country, reaching approximately 300 chief executives and other law enforcement partners.

## **Privacy**

As of March 2012, the National Network of Fusion Centers consisted of 77 primary and recognized fusion centers, as designated by state governors. By the end of March 2012, all of these fusion centers had developed privacy policies determined to be at least as comprehensive as the ISE Privacy Guidelines. The NSI PMO continues to work with fusion centers to implement the standards, policies, and processes of the NSI, so that they can share terrorism-related SARs with other participating NSI locations.

The CICC developed the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise* resource to assist agencies as they review and assess their policies and procedures related to privacy, civil rights, and civil liberties protections to ensure these policies are comprehensive and have been fully implemented. The template is recommended for use as a self-assessment tool within a law enforcement agency and is being used to promote peer-to-peer exchanges between similar intelligence enterprises. This peer-to-peer process will increase communication and coordination between agencies, identify smart practices, and provide feedback and recommendations to mitigate potential implementation gaps. In early 2010, the template was successfully piloted through a peer-to-peer exchange by the joint DHS/DOJ Fusion Process Technical Assistance Program between the Georgia Information Sharing and Analysis Center and the Florida Fusion Center.

Following this initial pilot and the development of the SAR Appendix, the NSI PMO, in collaboration with the DHS/DOJ Fusion Process Technical Assistance Program, offered the primary and designated fusion centers to undergo a peer-to-peer exchange to implement the *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*.

## Training

The NSI training strategy is a multifaceted approach designed to increase the effectiveness of SLTT law enforcement and public safety professionals and other frontline partners 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 appropriate agency implementation of the SAR process and to enhance a nationwide SAR capability. To achieve this goal, the NSI has developed and deployed training programs for frontline officers, analysts, chief executives, and hometown security partners regarding the behaviors and indicators of terrorism-related criminal activity.

State and local law enforcement agencies in Arizona and Georgia have worked to cultivate relationships with the Peace Officer Standards and Training (POST) associations to advance the SAR training message through the state POST requirements process.

### Hometown Security Partners

While continuing to provide high-quality training for the law enforcement community, the NSI has developed SAR awareness training for hometown security partners that are important to the SAR effort, including fire and emergency medical services personnel, public safety telecommunications professionals (e.g., 9-1-1 operators), emergency managers, corrections and probation and parole officers, and private sector security personnel and those charged with protecting the nation's critical infrastructure. The purpose is not to empower public safety officials to act on behalf of law enforcement but to have them understand the critical role they play in identifying and reporting suspicious activity to SLTT law enforcement.

9-1-1 is the number most people in the United States call to obtain help in a police, fire, or medical emergency, which uniquely affords 9-1-1 call-takers the opportunity to play an important role in SAR

awareness. The responsibilities of the emergency management community include working closely with operators and owners of critical infrastructure and key resources, responding to emergency situations, and gathering information about disasters, which may place them in unique positions to observe suspicious activity-related behaviors and indicators that, when viewed within the totality of circumstances, may indicate preoperational planning of a terrorist-related incident. Firefighters also have a significant reach into communities across America. In their efforts to prevent and respond to life and property losses, firefighters enter homes, businesses, vehicles, and other assets thousands of times each day and, as a result, may encounter behaviors and/or indicators of criminal activity. Community corrections professionals are also in a position to recognize criminal or potential terrorism activity, especially while this activity may be in the planning phase, due to their contact with offenders and families and friends of offenders. With more than 2 million security officers who protect our nation's critical infrastructure, these public safety and security professionals can be "force multipliers" to help recognize and report suspicious activity.

In order to ensure that this training was relevant for each of these specific sectors, the NSI PMO conducted a two-day focus group session consisting of subject-matter experts from these fields. The input provided by these experts was critical to the development of the training and will be an important factor in the rollout, which began in spring 2012. In particular, there were several associations that partnered with the NSI PMO, including:

- International Association of Fire Chiefs
- Association of Public-Safety Communications Officials
- National Emergency Management Association
- American Probation and Parole Association
- ASIS International
- National Association of Security Companies

The support and partnership from these associations is necessary for the success of the training package, and the NSI PMO will work with each of them over the coming year to help ensure that the training is pushed out to the memberships of each of these sectors.

#### **National Maritime Intelligence-Integration Office**

The National Maritime Intelligence-Integration Office (NMIO), in partnership with the NSI PMO, is bringing a SAR awareness training program that will focus on the maritime industry and the many individuals connected to port facilities. The purpose is not to empower port and private safety officials to act on behalf of law enforcement but to have them understand the critical role they play in identifying and reporting suspicious activity to SLTT law enforcement.

The United States conducts 95 percent of commercial trade via maritime conveyances—moving over 2 billion tons of freight a year and handling \$264 billion in annual commerce. The U.S. maritime responsibility includes 164,000 employees in water transportation and ports, 200,000 foreign sailors, 7 million cruise passengers, and 134 million ferry passengers. Including the management of the security

of the coastlines means there are over 25,000 miles of inland waterways, 95,000 miles of shoreline, 240-plus shipyards, and 1,000 harbor channels that need to be monitored.

NMIO and the NSI PMO plan to complete the development of the maritime industry sector training by the fall of 2012. The delivery of the new training module will be similar in format to other SAR Hometown Security Partners Training and will be accessed via familiar training portals and hard-copy CDs or DVDs. Additionally, the NSI PMO and NMIO are partnering with DHS, the United States Coast Guard, and the U.S. Department of Transportation's Maritime Administration (MARAD) to provide specialized presentations and discussions at ten ports across the nation. The intended outcome of these visits is to enhance the SAR business processes and ultimately capture a business process/model that can be replicated across the nation's ports. The training and port visits will serve to educate those professions within the maritime industry who have the best potential of being exposed to harbor-related indicators and behaviors associated with criminal and/or terrorist activity.

### **NSI Analyst Technical Assistance**

Contributing SAR information to the NSI Federated Search is only the first step to leveraging the value of the NSI Federated Search. The next step relates to the fusion center analysts' ability to search the shared information as part of the analytical process and to receive valuable information. To enhance this process, the NSI has developed an NSI Federated Search Tool Technical Assistance process for fusion center analysts. This technical assistance process provides analysts with the capability to quickly and effectively search for relevant information within the NSI Federated Search. This assistance will be primarily provided by the NSI Executive Support Specialists. The technical assistance offering lasts approximately four hours and will demonstrate how users can access the NSI Federated Search Tool via RISS and/or LEO and how to use the NSI Federated Search Tool. The technical assistance offering provides a live, thorough overview of the two primary search methods: the Single Line Search and the Advanced Search. It also includes an overview of the State and Local Anti-Terrorism Training (SLATT®) Database Search and the User Toolbar. Analysts will learn how to display the data in a geospatial format using the Map It/Link It tool. In addition to searching and mapping the data, the analysts will also learn how to save queries, set alert notifications, and locate contact information.

### **SAR Analyst Training**

Over the past year, the NSI PMO worked to deliver 24 analyst training sessions across the country, reaching almost 700 analysts. In addition, upon receiving authorization from the NSI PMO to conduct in-house SAR Analyst Training, DHS conducted three deliveries of the training in 2011. These sessions were well attended by personnel from nine DHS components, with a total of 83 people trained.

## Line Officer Training Update

The NSI PMO continued to make great strides in providing SAR training to law enforcement and support personnel to help ensure that they are trained to recognize behavior and incidents identified by law enforcement officials and counterterrorism experts from across the country as being reasonably indicative of criminal activity associated with terrorism. In particular, the support from the following associations has been key to delivering the training and receiving reporting numbers:

- Association of State Criminal Investigative Agencies
- International Association of Chiefs of Police
- Major Cities Chiefs Association
- Major County Sheriffs' Association
- National Fusion Center Association
- National Sheriffs' Association

Because of the efforts of those involved with these associations, the NSI PMO was able to increase the number of line officers trained to approximately 250,000 in 2011. NSI staff will continue to partner with and conduct outreach to these agencies in the coming year to increase that number, with the goal of reaching every line officer across the country.

### Georgia and Arizona POST Credit for NSI Line Officer Training

To help deliver the SAR Line Officer Training to all officers in a timely manner, state and local law enforcement agencies in Arizona and Georgia have worked to cultivate relationships with the Peace Officer Standards and Training (POST) associations to advance the SAR training message through the state POST requirements process. The Georgia Bureau of Investigation has made it possible for all line officers to receive POST credit for viewing the NSI Line Officer Training video as part of their annual in-service POST requirement and has also included the Criminal Intelligence Coordinating Council privacy training, *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety* video.

This was taken from testimony provided by the Executive Director of the National Fusion Center Association to the House Appropriations Subcommittee on Homeland Security.

A local police officer in Alabama made a traffic stop. Based on plain-sight observations, the officer asked to see the contents of a duffle bag in the back seat. Inside the duffle bag were four police uniforms and four police badges. When interviewed, each of the occupants stated they were headed to a location in Colorado, but each gave a different story. Beyond the traffic violation, there was no illegal activity, and the occupants were allowed to go on their way. What happened next shows how far we have come in taking proactive measures to protect the United States. The officer completed a report and clicked the "SAR" button available in the Alabama reporting system. That SAR went immediately to the Alabama Fusion Center, which analyzed the information and then contacted the fusion center in Colorado—the Colorado Information Analysis Center. Both of these fusion centers have an FBI presence.

As of April 2012, the matter of this incident is still being considered. Whether this situation has to do with terrorism or some other criminal activity, the key point is that within *HOURS*, federal, state, and local officials who can act to *PREVENT* criminal activity were aware of the situation. This goes far beyond information sharing—this is deep collaboration that makes our country safer, and the fusion centers enable it.

This action will lead to an increase in the number of officers in the state of Georgia who take the SAR Line Officer Training, as well as help to increase privacy protections. The same is expected in Arizona, where law enforcement has followed the lead set by Georgia and has made a submission to the Arizona POST Board for credit and curriculum approval. Arizona law enforcement officials are awaiting approval and hope to have the SAR Line Officer Training added soon to the cadre of training courses that are eligible to receive POST credits. The NSI will continue to facilitate the growth of the SAR training programs through both national POST contacts and states that adopt the program for state POST credits.

## **U.S. Department of Homeland Security—SAR Analytics**

### **DHS SAR Analysis Project**

The DHS SAR Analysis Project, which is managed by the Office of Intelligence and Analysis (I&A) Terrorist Targets and Tactics Branch, started as an effort to establish baseline metrics and evaluate the analytic value of the SAR in the NSI Federated Search. Since July 2011, the SAR team at DHS has conducted analysis and has begun developing a baseline of the reporting in the NSI for use in future analysis to assess any patterns, trends, tactics, techniques, and procedures. The analysts have been conducting a review and assessment of a representative sample of SAR information that was submitted through the NSI, including submissions made directly to the eGuardian system. This effort also advances DHS I&A all-source analysis, providing support for requests for information across DHS divisions, as well as external state and local support requests (SLSRs), NSI-derived production of Roll Call Releases, and support to other products, including joint-seal products with fusion centers.

### **DHS Roll Call Release Products Integrating SAR Data**

SAR information is currently being leveraged by both state and local law enforcement, as well as national security organizations, in an all-source analysis effort intended to help secure the homeland. A significant benefit of the NSI lies in making SAR readily available to analysts who can inform the interagency homeland security community about evolving trends and criminal schemes, collate reported data with current threat streams, and show nationwide aggregated metrics of SAR across regions and infrastructure sectors.

As part of this effort, DHS I&A is integrating SAR into the interagency “Roll Call Release” (RCR) product line to inform its customers of key issues relevant to homeland security. This one-page, for-official-use-only product, which is produced jointly with the FBI and the Interagency Threat Assessment and Coordination Group (ITACG), can be quickly read and presents key points to inform, highlight, and raise awareness of ongoing threats; general concepts of illicit activity; and documentation of actual incidents. RCRs are proving to be a viable intelligence product through which SAR information can be reported to various partners.

Several RCRs were released in the beginning of 2012 as part of a series that addresses the NSI-defined indicators and behaviors of potential terrorist preoperational attack planning. In addition to the NSI

definition and specific activities associated with the indicator and behavior, the RCRs also provide actual examples of SARs that were submitted to the NSI that illustrate these indicators and behaviors.

## Technology Improvements

The NSI PMO made several improvements to the NSI Federated Search over the past year and has also provided resources for users to turn to for assistance, if needed.

### Single Line Search

Similar to a Google search, the NSI Federated Search Tool provides a user with the ability to enter search parameters in an unstructured entry called the Single Line Search. In addition, the Single Line Search provides broader search parameters than previously available on the Advanced NSI Search Tool, which will help analysts find the information they need in a more efficient, expedient manner. A review of how to input search terms into the Single Line Search has been included in the NSI Analyst Technical Assistance that is provided by the Executive Support Specialists, and instructions are also provided in the updated NSI Federated Search User Manual.

### Subscription Service

NSI Federated Search users can now create and save queries, also known as a subscription service, by utilizing the NSI user console. These queries can be saved to run on a recurring basis, identify other users searching the same criteria, and identify when a new SAR is submitted that contains the information saved in the data query. The user console can be accessed from any NSI search or results screen. Detailed instructions and examples of the subscription service feature are provided in the updated NSI Federated Search User Manual.

### NSI Analytics

One reason the NSI Federated Search was developed was to share SARs and allow fusion centers, the FBI, and other agencies to review shared SARs so that analysts could potentially link behaviors and activities together with current threat information in an effort to prevent terrorism. As the NSI program expanded and input was received from the users of the NSI Federated Search Tool, a demand arose for the ability to view SAR at a higher level than searching a specific set of terms or criteria. To address this desire from the field and make the data being provided by all the NSI partners more user-friendly, an NSI Analytical Tool has been developed and will be released in 2012. This tool allows NSI users to:

- Review all SAR information submitted by each fusion center as an NSI Summary. These can be viewed by activity, threat, and/or infrastructure.
- Review SARs for a specific fusion center by activity, threat, and infrastructure.

- Search SARs for one or multiple activity types, threat codes, and/or infrastructure codes. This search will inform the user about the number of SARs that can be viewed based on the different combinations of items selected, allowing the user to select a combination of items and view all the SAR information that resulted from that combination.
- Compare across multiple NSI users for a specific activity, threat, or infrastructure.
- View a summary of what types of SARs a fusion center is handling based on activity, threat, or infrastructure.

### **Shared Space—eGuardian Information Sharing— eGuardian Web Service**

In an attempt to bring all the facets of the NSI program together, the NSI PMO, working in conjunction with the eGuardian staff, has implemented a capability so that fusion centers electronically push NSI SAR from the fusion centers' local NSI common box to the FBI's eGuardian system. This migration was done by utilizing the eGuardian Web service, which enables not only the push of an NSI SAR to eGuardian but also the immediate receipt of an eGuardian identification number for future reference.

Based on the feedback from fusion center directors, the NSI implemented a technical ability for a fusion center to push SAR information not only to the NSI Federated Search but simultaneously to eGuardian within a very short time of the fusion center's decision to share that NSI SAR.

In May 2010, the FBI's Virtual Threat Analysis Center (VTAC) received a tip from the Barnesville, Georgia, Police Department that an unknown caller was making bomb threats. This information was entered into eGuardian, and then, through an automated process, the incident was placed into Guardian. A full investigation was initiated by FBI Atlanta, Macon Resident Agency, special agents, and within 72 hours, Satish Kumar Patel was arrested. Mr. Patel was charged with three counts of false public alarm, domestic terrorism, four counts of terroristic threats, and two counts of unlawful conduct during an emergency call. He pled guilty to three counts of making threats to damage buildings by means of fire or explosives.

### **NSI Help Desk**

The NSI Help Desk and Knowledge Base is a secure site that allows users to find information regarding frequently asked questions (FAQs) pertaining to the NSI program. Through this site, users can search a database of SAR-related FAQs, submit additional FAQs to the database, find helpful links and points of contact, view training documents and podcasts, and request additional assistance from the Help Desk.

### **Frequently Asked Questions**

The FAQs—commonly asked SAR-related questions and answers—may be technical, procedural, or policy-oriented in nature. Examples of FAQ topics include but are not limited to Federated Search; baseline capabilities; privacy, civil rights, and civil liberties compliance; standard operating procedures and guidelines for fusion centers; Information Exchange Package Documentation (IEPD); NIEM; fusion

center technical assistance; and predictive analytics. FAQs are often submitted to the NSI Help Desk but may also be submitted to the NSI PMO and support team through e-mails, calls, letters, and requests for technical assistance.

### **Conclusion**

The NSI has continued to make major improvements in sharing terrorism-related information across the country, mostly due to the many federal, state, local, tribal, and territorial partners, national and international law enforcement associations, and reaching out beyond the law enforcement community to include new stakeholders to the overall mission. This was evidenced by the release of the Unified Message, which provides a clear message to the field that there is a single, coordinated effort to encourage the reporting of suspicious activity and to share this information with the departments and agencies that need it to help keep our country safe from terrorism. The endorsement of this document by a wide cross-section of key departments, national and international associations, and major agencies is an enormous accomplishment.

The addition of the NSI PMO Executive Support Specialists has been crucial in the advanced deployment of the NSI. Their expertise and hands-on support to NSI sites across the country have allowed fusion centers to expedite implementation of NSI processes and has allowed the NSI PMO to exceed expectations on deployment.

The NSI PMO expanded partnerships, developing many relationships with public safety organizations and associations which have helped promote and endorse the NSI, particularly with the SAR Hometown Security Partners Training. Based upon this past year's progress, the NSI plans to expand its partnerships to other public safety agencies and organizations while continuing to maintain the existing relationships with those who have supported the mission since the beginning.

The NSI PMO is enthusiastic to build upon the hard work and foundations established in the past year and looks forward to the successes of the future.

## Appendix 1—Resources

NSI and SAR-related resources can be accessed at <http://nsi.ncirc.gov/resources.aspx>.

### [NSI Overview](#)

Provides an overview of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).

### [Unified Message](#)

This Unified Message document, issued in April 2012, was created to help clarify a unified approach to the process of reporting and sharing information related to suspicious activity.

### [NSI Training Overview](#)

Provides a description of the multifaceted approach to the NSI training strategy, which includes training programs for frontline officers, analysts, and chief executives, as well as SAR awareness training for partners with similar missions to those of law enforcement constituencies.

### [NSI Hometown Security Partners](#)

This document is an overview of the SAR Hometown Security Partners Training strategy, which provides SAR awareness training for partners with similar missions to those of law enforcement constituencies, or "hometown security partners."

### [NSI Technology Fact Sheet](#)

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

### [\*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 which serve as a foundational element of the NSI and which are required to participate.

### [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.

[\*Suspicious Activity Reporting Process Implementation Checklist\*](#)

Provides a simplified checklist for chief executives and senior leadership to implement a SAR process within their agencies.

[\*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.

[\*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**

[\*Nationwide SAR Initiative Annual Report 2010\*](#)

This report provides an overview of the first 12 months of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) and features the program's foundation, success, and future growth.

[\*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 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**

[NSI Privacy Fact Sheet](#)

This fact sheet provides an overview of the various components of the NSI Privacy Protection Framework, which is an integral element to the protection of privacy throughout the SAR process and to the overall success of the NSI.

[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.

[The Nationwide Suspicious Activity \(SAR\) Reporting Initiative \(NSI\) Privacy, Civil Rights, and Civil Liberties Analysis and Recommendations](#)

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 which serve as a foundational element of the NSI and which are required to participate.

## Technology Resources

### [NSI Technology Fact Sheet](#)

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

### [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.

### [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.

### [eGuardian Privacy Impact Assessment](#)

## Training Resources

### [LEAPS.TV Overview](#)

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<sup>SM</sup>) 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](#).

### [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 was developed in partnership with select sites that participated in the Nationwide SAR Initiative (NSI) Evaluation Environment.

### [Building Communities of Trust: A Guidance for Community Leaders](#)

This document is a complementary piece to the *Guidance for Building Communities of Trust*, and was developed to assist community leaders working with law enforcement agencies to facilitate dialogue and discuss ways to work together to prevent crime and terrorism.

### [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](#).

### **Appendix 3—Unified Message**

*A Call to Action: A Unified Message Regarding the Need to Support Suspicious Activity Reporting and Training* is included on the following two pages.

# A CALL TO ACTION:

## A UNIFIED MESSAGE REGARDING THE NEED TO SUPPORT SUSPICIOUS ACTIVITY REPORTING AND TRAINING

Efforts to address crime and threats in our communities are most effective when they involve strong collaboration between law enforcement and the communities and citizens they serve. As a law enforcement or homeland security professional, you understand that *Homeland Security Is Hometown Security*.<sup>1</sup> Local, state, tribal, territorial, campus, and federal representatives are united in efforts to make our country safer.

One of these efforts relates to Suspicious Activity Reporting. To address this issue, in 2011, the International Association of Chiefs of Police (IACP) hosted a meeting of representatives from numerous local, state, and federal agencies and law enforcement organizations to create a unified approach to reporting and sharing suspicious activity.

As a result, these leaders have partnered to support a strategy that will unify the efforts of all agencies and organizations involved in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The overall effort focuses on (1) increasing public awareness of reporting suspicious activity to law enforcement, (2) generating Suspicious Activity Reports by law enforcement, (3) analysis conducted by fusion centers and Federal Bureau of Investigation (FBI) Field Intelligence Groups (FIGs), and (4) investigation by the FBI's Joint Terrorism Task Forces (JTTFs).

*As a law enforcement or homeland security professional, you are responsible to ensure that the public you serve understands how to report suspicious activity and that your agency/organizational members support the collection, analysis, and submission of Suspicious Activity Reports to your fusion center or FBI/JTTFs.*

Fusion centers, FIGs, and JTTFs will share Suspicious Activity Reports seamlessly. The NSI Program Management Office (NSI PMO) and the FBI made technical adjustments in 2011 to ensure interoperability between the eGuardian and Shared Space systems. Suspicious Activity Reports entered into either system will be expeditiously pushed into the other automatically for sharing with other partners within the NSI as appropriate.

Detailed below are key points and action items that all law enforcement and homeland security personnel should be aware of, support, and institutionalize within their area of responsibility:

### REPORTING SUSPICIOUS ACTIVITIES

- ◀ Agencies at all levels of government should utilize the "If You See Something, Say Something™" program to raise public awareness of indicators of terrorism and to emphasize the importance of reporting suspicious activity to the proper law enforcement authorities, while protecting privacy, civil rights, and civil liberties. (See "Outreach Activities" below for more details.)
- ◀ The public should contact law enforcement via 9-1-1 when an immediate response is needed regarding suspicious activity for any type of crime, including terrorism.
- ◀ Personnel from your agency should prepare Suspicious Activity Reports and forward them to fusion centers or FBI/JTTFs for follow-up and mutual coordination/deconfliction.
- ◀ Other potentially terrorism-related tips or leads reported directly to FBI/JTTFs will be evaluated for investigation, coordination, and entry into the NSI as appropriate.

<sup>1</sup> From *Hometown Security to Homeland Security*, IACP's Principles for a Locally Designed and Nationally Coordinated Homeland Security Strategy, International Association of Chiefs of Police, <http://www.theiacp.org/LinkClick.aspx?fileticket=78X8uKjLa0U%3D&tabid=392>.



## NATIONWIDE SUSPICIOUS ACTIVITY REPORTING (SAR) INITIATIVE (NSI)

- ◀ The NSI establishes standardized processes and policies that provide the capability for local, state, tribal, territorial, campus, and federal law enforcement to share timely, relevant Suspicious Activity Reports while working to ensure that privacy, civil rights, and civil liberties are protected.
- ◀ There are multiple options for entry of Suspicious Activity Reports.

## SAR TRAINING

- ◀ It is important to ensure that your agency's personnel have received the frontline officer training on identifying and reporting those behaviors that are potentially indicative of terrorist or other criminal activity while emphasizing the protection of privacy, civil rights, and civil liberties. This training is coordinated by the NSI, the U.S. Department of Homeland Security (DHS), the FBI, the IACP, and others for nationwide implementation and is available online via these sites:
  - NSI Web site: <http://nsi.ncirc.gov/sarlot/>
  - LEAPS.TV: [http://www.leaps.tv/programdetail.php?program\\_code=201008031500](http://www.leaps.tv/programdetail.php?program_code=201008031500)
  - MIPT: <http://www.mipt.org/SARTraining.aspx>

*It is vitally important that law enforcement agencies conduct SAR training with all law enforcement personnel, including supervisors, and document completion. Officers, chiefs, sheriffs, training officials, and other executives should integrate SAR training into initial and recurring training curricula.*

## FUSION CENTERS, FIGS, AND JTTFS

- ◀ Fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among local, state, tribal, territorial, and federal partners. They produce actionable intelligence for dissemination, which can aid other law enforcement organizations, including the JTTFs, in their investigative operations.
- ◀ JTTFs are multiagency task forces designed to combine the resources, talents, skills, and knowledge of local, state, tribal, territorial, and federal law enforcement, as well as the Intelligence Community, into a single team that investigates and/or responds to terrorist threats. JTTFs investigate Suspicious Activity Reports and other terrorism tips and leads.
- ◀ FIGs, the hub of the FBI's intelligence program in the field, are the primary mechanism through which field offices identify, evaluate, and prioritize threats within their territories. Using dissemination protocols, FIGs contribute to regional and local perspectives on threats and serve as an important link between fusion centers, the FBI/JTTFs, and the Intelligence Community.

## OUTREACH ACTIVITIES

- ◀ The "If You See Something, Say Something™" public awareness campaign is a simple and effective program to raise public awareness of indicators of terrorism and violent crime.
- ◀ DHS uses "If You See Something, Say Something™" with permission from the New York Metropolitan Transportation Authority. Agencies, companies, or groups interested in partnering with DHS on this campaign should contact the DHS Office of Public Affairs at (202) 282-8010.

