Cohesive communities are safer communities, and community cohesion starts with trust. The recommendations and resources in this guidebook can help you be more proactive in working with your law enforcement agencies and fellow community members to help build that trust. Through active communication and participation at the grassroots level, communities are better prepared to deal with and prevent threats of crime, violent extremism, and terrorism.

ADDITIONAL RESOURCES

The ***Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Web site*** includes more detailed information about the NSI as well as links to other resources and descriptions of training. See http://nsi.ncirc.gov.

Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Functional Standard Version 1.5 builds on, 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. That document is available at http://nsi.ncirc.gov/documents/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf .

The ***U.S. Department of Homeland Security*** provides additional details about fusion centers at www.dhs.gov/fusioncenters.

Fusion Center Guidelines aid in the development and operation of fusion centers. The guidelines assist in addressing common obstacles in developing and operating a fusion center and guide administrators in developing policies, managing resources, and evaluating services. See http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

Baseline Capabilities for State and Major Urban Area Fusion Centers identify the baseline capabilities for fusion centers and the operational standards necessary to achieve each of the capabilities. This document is located at http://it.ojp.gov/documents/baselinecapabilitiesa.pdf.

Guidance for Building Communities of Trust 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. This document is located at http://nsi.ncirc.gov/documents.

"***If You See Something, Say Something™***" is a public awareness campaign, created by the New York Metropolitan Transportation Authority and launched nationally by the U.S. Department of Homeland Security in 2010. This campaign is a simple and effective way to raise public awareness of indicators of terrorism and terrorism-related crime and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities. For more information on the "If You See Something, Say Something™" campaign, visit http://www.dhs.gov/IfYouSeeSomethingSaySomething.

The ***Office of Community Oriented Policing Services (COPS)*** Web site, www.cops.usdoj.gov, can provide more information on community policing.

The ***Community Policing Defined*** guidebook provides a detailed description of the elements and subelements that comprise the community policing philosophy. The document describes the range of collaborative partnerships that exist between policing agencies and the individuals and organizations they serve; it outlines the process of how they go about engaging in the proactive and systematic examination of identified problems to develop effective responses; and it illustrates how they align their organizational management, structure, personnel, and information systems to support community partnerships and proactive problem-solving. http://cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=513.

The ***U.S. Department of Justice Community Relations Service*** works with communities to employ strategies to prevent and respond to alleged violent hate crimes committed on the basis of actual or perceived race, color, national origin, gender, gender identity, sexual orientation, religion, or disability.

APPENDIX A. NSI Overview

NSI OVERVIEW

Every day, law enforcement officers at all levels of government—state, local, tribal, and federal—observe suspicious behaviors or receive reports of suspicious activity, either from concerned citizens or businesses. Although an action or activity reported may not seem significant, when combined with other similar actions or activities, it may become an essential element in preventing criminal or even terrorist activity.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) Program Management Office (PMO) initiated operations in March 2010 with the 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. The NSI has worked hard to incorporate the informal processes that traditionally exist within law enforcement agencies into the standards, policies, and processes developed by the NSI that allow law enforcement agencies to easily share information with the critical partners that need it to help prevent terrorist attacks.

The NSI has developed a comprehensive program that includes community and law enforcement outreach, standardized processes, training, a privacy framework, and enabling technology, all of which are essential for successful implementation of the NSI. Through strong leadership and outreach, the NSI PMO has continued working with key partners at the state, local, tribal, territorial, and federal levels of government, as well as advocacy groups, to not only develop and update the policies and processes of the NSI but also help ensure that Americans' privacy, civil rights, and civil liberties are protected throughout implementation and

TRAINING

The NSI training strategy is 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 training is broken down into focus areas for the Frontline Officer, Analyst, Executive, and Hometown Partners, with each training focusing on the various law enforcement professionals and their respective level of responsibilities and duties.

FRONTLINE OFFICER

The SAR Line Officer Training focuses on the critical role frontline officers have in the effective implementation of the SAR process by identifying and documenting suspicious activity. The NSI PMO, with support from the International Association of Chiefs of Police, the Major County Sheriffs' Association, the Major Cities Chiefs Association, and the National Sheriffs' Association, is working to deliver the 15-minute training video to all law enforcement and support personnel across the country.

ANALYST

The SAR Analytic Role Training is designed to increase the awareness of the NSI by enhancing fusion center analysts' understanding of behaviors and indicators indicative of terrorism activities while also highlighting the importance of protecting privacy, civil rights, and civil liberties as information is documented, vetted, and shared nationwide.

EXECUTIVE BRIEFING

The SAR Executive Briefings focus on executive leadership, policy development, privacy and civil liberties protections, agency training, and community outreach. Hometown Partners

HOMETOWN PARTNERS

The soon-to-be-released SAR Hometown Security Partners Training will provide SAR awareness for other key non-law enforcement constituencies, or "hometown security partners," such as public safety and those charged with protecting the nation's critical infrastructure, who are important to the SAR effort.

PRIVACY, CIVIL RIGHTS, CIVIL LIBERTIES

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 various advocacy groups, such as the American Civil Liberties Union, to develop protections that, when consolidated, make up a comprehensive NSI Privacy Framework. The NSI requires each fusion center to consider privacy throughout the SAR process by fully adopting this framework prior to NSI participation. Working with these different advocacy groups and major stakeholders in states across the country has served an important role in successfully shaping NSI policies and processes.

COMMUNITY OUTREACH AND AWARENESS

The Building Communities of Trust (BCOT) initiative focuses on developing relationships of trust between law enforcement, fusion centers, and the communities they serve—particularly immigrant and minority communities—to help prevent crime and/or terrorist-related activities and keep our communities safe.

In July 2010, the U.S. Department of Homeland Security (DHS), at Secretary Janet Napolitano's direction, launched a national "If You See Something, Say Something™" public awareness campaign—a simple and effective program to raise public awareness of indicators of terrorism and violent crime and to emphasize the importance of reporting suspicious activity to the proper state or local law enforcement authorities. This campaign is being launched in conjunction with NSI rollout sites, with both programs underscoring the concept that homeland security begins with hometown security, where an alert public plays a critical role in keeping our nation safe.

STAKEHOLDER OUTREACH

The NSI is a collaborative effort of federal, state, local, and tribal agencies, along with a number of law enforcement organizations across the country, working hand-in-hand to advocate the importance of the NSI. The efforts of these organizations—the International Association of Chiefs of Police, the Major Cities Chiefs Association, the Major County Sheriffs' Association, and the National Sheriffs' Association—have provided ongoing support and input to the development and implementation of the NSI by promoting the SAR training and by inviting the NSI to participate in conferences where the NSI message can be delivered to state and local law enforcement agencies.

TECHNOLOGY

Technology plays a vital role in the NSI process. In order for the information to be shared across the country, each agency must have a process and a system in place to send and receive these suspicious activity reports (SARs). To support the operational mission, the NSI has leveraged the National Information Exchange Model (NIEM), which allows the interoperability and seamless exchange of SAR information.

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) in the future. Regardless of what mechanism is used to receive the information, the NSI was developed to ensure that information received and vetted at a fusion center will be quickly reviewed by the FBI's Joint Terrorism Task Forces (JTTF) for possible investigation and shared with a host of analysts for the purpose of analytical pursuits.

QUESTIONS?

For more on the NSI, please visit nsi.ncirc.gov. Or, contact the NSI Program Management Office at nsipmo@usdoj.gov (202) 514-0617.

APPENDIX B. ISE-SAR Functional Standard 1.5

PART B- ISE SAR CRITERIA GUIDANCE CHART

Category	Description
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).
Sabotage/Tampering/ Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/ infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.

POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION[11]	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

[11] Note: These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may used as specific suspect descriptions).

APPENDIX C. Privacy Guidelines

State and major urban area fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.

Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line homeland security and law enforcement partners to understand local implications of national intelligence, thus enabling local officials to better protect their communities.

MILESTONE FOR PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

Both fusion center directors and the federal government have identified the protection of privacy, civil rights, and civil liberties as a key priority and an important enabling capability to ensure that fusion centers protect the legal rights of Americans while supporting homeland security efforts. It is critical that fusion center personnel not only receive training to understand the need to protect privacy, civil rights, and civil liberties, but also have a policy in place clearly outlining how this will be achieved.

To help with these efforts, the DHS Privacy Office, working in collaboration with the DHS Office of Intelligence and Analysis (I&A), DHS Office of Civil Rights and Civil Liberties, DOJ Privacy Office, and the Program Manager of the Information Sharing Environment, began an independent review in November 2009 of fusion center privacy policies. Today, all fusion centers have successfully completed this important step and received letters from the DHS Chief Privacy Officer stating that these policies have been determined to be at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines.

The completion of these privacy policies by all fusion centers is a milestone to support the sharing of terrorism and other homeland security information between the federal government and fusion centers during situations involving time-sensitive and emerging threats.

PROTECTING PRIVACY WHILE SHARING INFORMATION

Established by the *Intelligence Reform* and *Terrorism Prevention Act of 2004*, the ISE provides analysts, operators, and investigators with integrated and synthesized terrorism, weapons of mass destruction, and homeland security information needed to enhance national security and help keep our nation safe.

The law required the President to issue guidelines to protect privacy and civil liberties. From this, the *ISE Privacy Guidelines* were established to help ensure that ISE sharing partners sufficiently protect Americans' privacy and civil liberties while sharing important terrorism and homeland security information.

These guidelines require that ISE participants—such as the National Network of Fusion Centers—have a written privacy protection policy that is "at least as comprehensive" as the ISE Privacy Guidelines. For example, within each privacy policy, fusion centers must identify a privacy officer and clearly articulate the security measures in place to protect personally identifiable information.

NEXT STEPS

The DHS Privacy Office remains engaged with the fusion centers as they work to implement their privacy policies. In partnership with the DHS Office for Civil Rights and Civil Liberties, I&A, and DOJ, the DHS Privacy Office will continue to provide support to the National Network of Fusion Centers to help ensure that these policies are adhered to, as well as to provide customized privacy, civil liberties, and civil rights training to those working in this arena, including the following:

1. DHS intelligence officers assigned to a fusion center.
2. State and major urban area fusion center personnel.
3. Individuals serving as privacy officers in fusion centers.

APPENDIX D. Communities' Frequently Asked Questions About NSI and Fusion Centers

BUILDING COMMUNITIES OF TRUST

What is the Building Communities of Trust Initiative?

The Building Communities of Trust Initiative focuses on developing relationships of trust among law enforcement, fusion centers, and the communities they serve, particularly immigrant and minority communities, to address the challenges of crime and terrorism. By fostering relationships, involving the community in the course of privacy policy development and implementation, 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 indicate criminal activity. The Building Communities of Trust Initiative is an effort to reach out to various cities around the country to help clear up misunderstandings about law enforcement and community roles and also to give communities a chance to express their thoughts and concerns. This initiative included a series of facilitated sessions that convened privacy, civil rights and civil liberties groups, community leaders, and law enforcement officials for an intensive dialogue focused on developing understanding and trust.

What is the role of the U.S. Attorneys in working with their districts to help protect communities from violent crimes and terrorism?

U.S. Attorneys offices are the lead federal law enforcement representative with the mission of supporting engagement with communities. They are available to discuss issues such as civil rights, counterterrorism security measures, international events, foreign policy, and other community concerns; raise awareness about the threat of violent extremism; and also facilitate partnerships to help identify and prevent radicalization to violence. The types of communities involved in engagement differ depending on jurisdictions across the country. U. S. Attorneys, in consultation with local and Federal partners, are best positioned to make local determinations on how best to engage community leaders.

SUSPICIOUS ACTIVITY REPORTING

What is the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)?

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is an effort to establish a standardized nationwide capacity for gathering, documenting, processing, analyzing, storing, and sharing terrorism-related suspicious activity reports in a manner that rigorously protects the privacy, civil rights, and civil liberties of all Americans.[12]

What is a suspicious activity report?

A suspicious activity report is official documentation of observed behavior which reasonably indicates preoperational planning related to terrorism or other criminal activity.

What are the suspicious activities that should be reported?

Examples of activity to be reported include, but are not limited to, surveillance, photography of facilities, site breach or physical intrusion, cyberattacks, possible testing of security or security response, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemicals or toxic materials, or other unusual behavior or incidents. Further details can be found in the ISE-SAR Criteria Guidance in Appendix B.

How does a person report a suspicious activity?

If a person observes a crime in progress or other emergency activity, he or she should call 9-1-1. There are numerous other ways to report suspicious activity, which is not an emergency by nature, and these vary by jurisdiction. Other methods include tip lines and Web sites, as well as something as informal as contacting a trusted law enforcement partner. Community members are encouraged to contact their local law enforcement agencies to find out the ways to report in their communities.

Where does a report of suspicious activity go when it is reported?

The information is reviewed within a local or federal agency by trained analysts for linkages to other suspicious or criminal activity. Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies

---

[12] For detailed information about the Nationwide Suspicious Activity Reporting Initiative, see http://nsi.ncirc.gov/.

may forward most SARs directly to the relevant state or major urban area fusion center or a Joint Terrorism Task Force (JTTF) with minimal local processing. Larger cities, on the other hand, may have trained counterterrorism experts on staff that apply a more rigorous, analytic review of the initial reports and filter out those that can be determined not to have a potential terrorism nexus.

After appropriate local processing, agencies make SAR information available to the relevant state or major urban area fusion center. Depending on the nature of the activity, the information could cross the threshold of "suspicious" and move immediately into law enforcement operations channels for follow-on action against the identified terrorist activity. In those cases where the local agency can determine that an activity has a direct connection to criminal activity associated with terrorism, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

The fusion center or federal agency enters the SAR into its local information system and then performs an additional analytic review to establish or discount a potential terrorism nexus. Based on this review, the officer or analyst determines whether the information has a potential nexus to terrorism. If the officer or analyst cannot make this explicit determination, the report will not be accessible by other authorized law enforcement or homeland security personnel, although it may be retained in local fusion center or federal agency files in accordance with established retention policies.

Once the determination of a potential terrorism nexus is made, the suspicious activity report is stored where it can be accessed by authorized law enforcement and homeland security personnel in the state or major urban area fusion center's area of responsibility. Although the information is accessible by other appropriate law enforcement and homeland security personnel, it remains under the control of the submitting organization.

Once these suspicious activity reports are accessible, they can be used to support a range of counterterrorism analytic and operational activities. This step involves the actions necessary to integrate this information into existing counterterrorism analytic and operational processes, including efforts to "connect the dots," identify information gaps, and develop formal analytic products.

What happens to reports where an activity or a person is deemed not to be suspicious or is added maliciously to the SAR database?

Operational feedback on the status of suspicious activity reports is an essential element of an effective NSI process with important implications for privacy and civil liberties. The process supports notification of all participants when further evidence determines that a suspicious activity report was designated incorrectly so that the original information does not continue to be used as the basis for analysis or action.

What type of training do law enforcement agencies receive to implement the NSI?

There are currently three levels of training for agencies participating in the NSI.[13]

Executive Briefings—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.

Analytic Training—Ensuring that suspicious activity reports are 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 to identify behaviors that may be associated with pre-incident terrorism planning and the process for sharing terrorism-related SAR 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 is delivered in an eight-hour workshop format.

Line Officer Training—Front-line law enforcement personnel are trained to recognize behavior and incidents that may indicate criminal activity associated with terrorism. Their routine duties position them to observe and report suspicious behaviors or activities. The SAR Line Officer Training, which can be taken online, focuses on the critical role line officers have in the effective implementation of the SAR process by identifying and documenting suspicious activity.

---

[13] http://nsi.ncirc.gov/training.aspx.

Our problem is violence, guns, gangs, and drugs. How does the NSI help us to address those issues?

While the NSI is focused on behaviors that may indicate terrorist activity, relationships developed by law enforcement and the community through the BCOT initiative can affect other information sharing efforts between law enforcement and the community. Additionally, information provided may not have a connection to terrorism but may have a connection to other crime in the community. Fusion centers help ensure that information received regarding other crimes is first analyzed (if appropriate), and then referred to the responsible local law enforcement agency.

What is the redress procedure if someone's name is wrongly included in a SAR?

Law enforcement agencies and fusion centers have redress procedures, which vary from jurisdiction to jurisdiction. If a person feels that his or her privacy, civil rights, or civil liberties were violated, he or she should contact the local law enforcement agency or fusion center.

How can this process be implemented in a manner which respects community values?

Privacy policies are customized by each fusion center in accordance with local and state laws. Fusion centers and local law enforcement agencies are also encouraged to involve the community in the development of privacy policies that reflect the community's values.

Is information about juveniles treated differently than information about adults?

The NSI focuses on behaviors, not on individuals, and does not distinguish between adults and minors.

STATE AND MAJOR URBAN AREA FUSION CENTERS

What is a fusion center?

State and major urban area fusion centers serve as focal points within states and local environment for the receipt, analysis, gathering, and dissemination of threat-related information among the federal government, state, local, tribal, territorial, and private sector partners. Fusion centers facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

What is the role of a fusion center in the NSI process?

Fusion centers play an integral role in the NSI process. Trained fusion center analysts review suspicious activity reports to determine whether they have a connection to criminal or terrorist activity. Analysts forward terrorism-related information, which is made accessible to other authorized law enforcement and homeland security personnel. They also forward criminal and terrorism-related information directly to law enforcement agencies, such as gang task forces or Joint Terrorism Task Forces, for investigation. Finally, fusion centers use these suspicious activity reports to develop local products that address the potential threat of crime groups or potential crime or terrorist activities in their areas.

Which agencies are represented at a fusion center?

There is no one model for fusion center representation. Each fusion center determines the makeup of its center based on local needs and available resources. Fusion centers generally include state, local, tribal, and territorial law enforcement agencies, federal homeland security and law enforcement partners such as the U.S. Department of Homeland Security and the Federal Bureau of Investigation, and other public safety disciplines such as the fire service, as well as private sector partners.

Are there any standards with which fusion centers must comply?

Yes. The U.S. Department of Justice's Global Justice Information Sharing Initiative's Fusion Center Guidelines provide guidance to ensure that fusion centers are established and operated consistently across the country.[14]

The *Baseline Capabilities for Fusion Centers* are a supplement to the *Fusion Center Guidelines* and identify the capabilities and standards necessary for a fusion center to be considered capable of performing basic functions. By achieving this baseline level of capability, a fusion center will have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information. This baseline level of capability will support specific operational capabilities, such as Suspicious Activity Reporting (SAR); alerts, warnings, and notifications; risk assessments; and situational awareness reporting.[15]

---

[14] U.S. Department of Justice, *Fusion Center Guidelines,* http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

[15] U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers*, http://it.ojp.gov/documents/baselinecapabilitiesa.pdf.

CIVIL RIGHTS, CIVIL LIBERTIES, AND PRIVACY

How is privacy protected by a fusion center?

Each fusion center is required to adopt a privacy, civil rights, and civil liberties policy (privacy policy), a written, published statement that articulates the center's position on how it handles the personally identifiable information and other personal, sensitive information it seeks or receives and uses in the normal course of business. The purpose of a privacy policy is to articulate within the center, to external agencies that access and share information with the center, to other entities, and publicly that the center will adhere to legal requirements and center policy and procedural provisions that enable gathering and sharing of information to occur in a manner that protects constitutional rights, including personal privacy and other civil liberties, and civil rights.

How are law enforcement officers trained on diversity issues?

Different agencies have their own standards and training protocols regarding cultural diversity. The NSI encourages the community to reach out to its local law enforcement agency to see what is offered in the community.

How do we ensure that communications about reporting suspicious activities are culturally sensitive and do not result in racial profiling?

The NSI focuses on behaviors, not on individuals. The functional standard outlines those behaviors that can serve as the basis for a suspicious activity report. Training reinforces the notion that suspicious activity reports should not be based on religions, race, or any other inappropriate factor.

NOTES

NOTES

- **Share crime prevention and terrorism related information with community members through meetings, presentations, Web sites, community newsletters, and social media.** By sharing your knowledge and concern for public safety with your fellow community members, you can educate them on identifying suspicious activity and help build trust in law enforcement.

- **Host cultural awareness trainings and events.** These events will allow law enforcement and community members to learn more about the various cultures and needs in the community in order to build trust and prevent misunderstandings or biased reports.

- **Participate in law enforcement volunteer programs such as Volunteers in Police Service and Neighborhood Watch/USAonWatch.** Volunteer programs can enable you to be extra eyes and ears in your community and help you provide ongoing support to your local law enforcement agency.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

515 North Washington Street

Alexandria, VA 22314

1-800-THE-IACP

www.theiacp.org