Nationwide Suspicious Activity Reporting

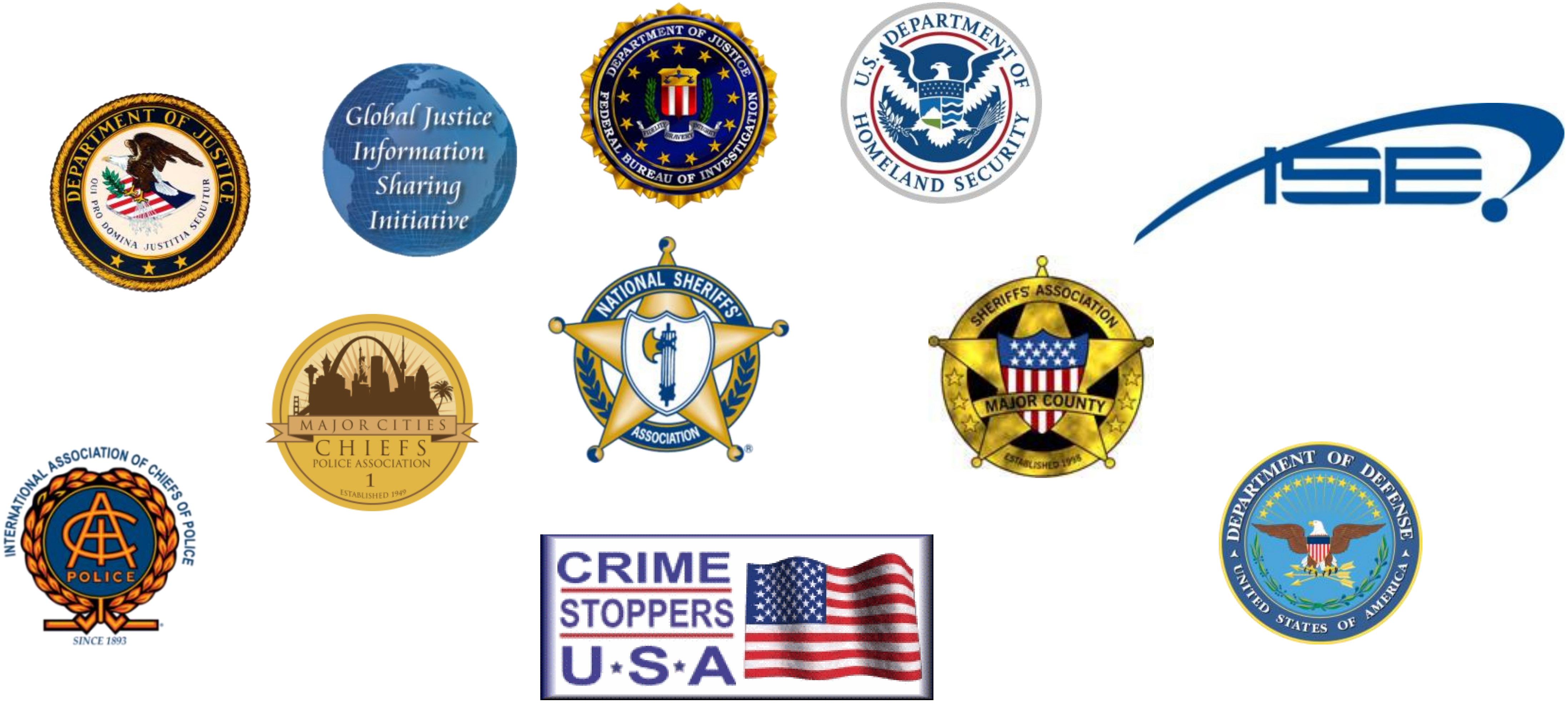
Crime Stoppers USA Training Conference
New Orleans
September 2018

NATIONWIDE SAR
NSI
INITIATIVE

Annual Training Conference
New Orleans, LA
September 9-12, 2018

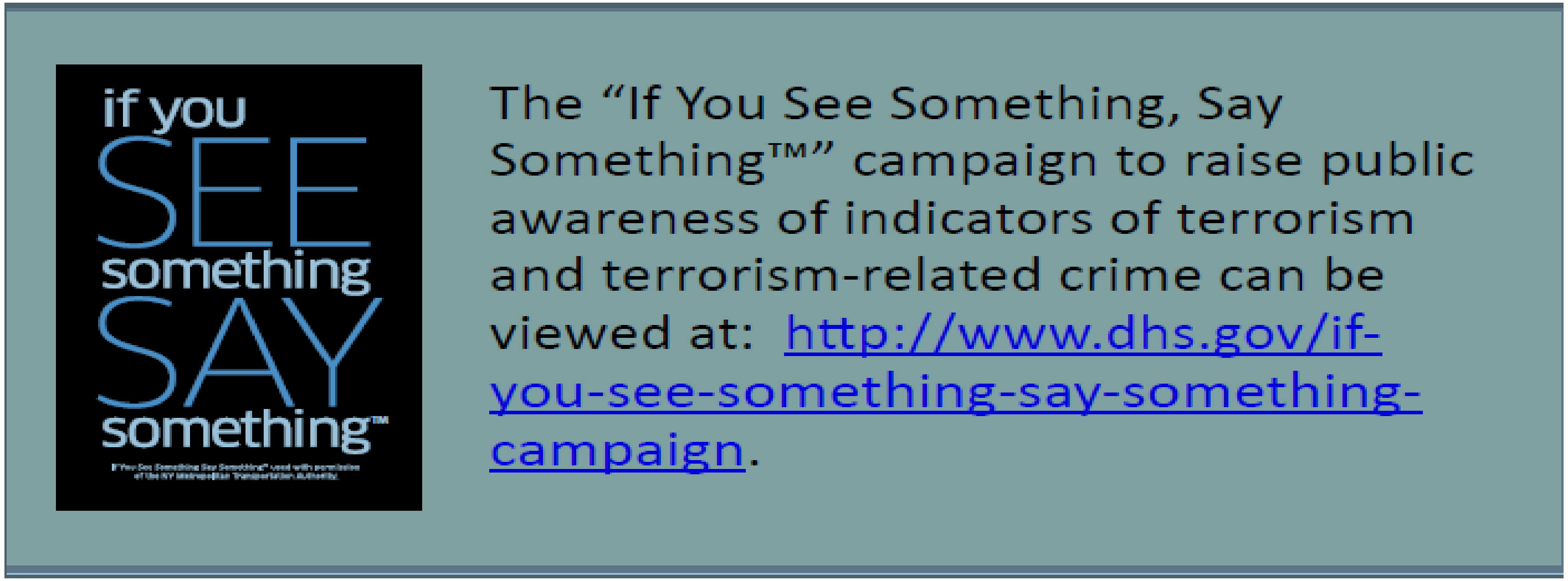
Hosted by: CRIMESTOPPERS GNO

NSI Project Partners


DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
Global Justice Information Sharing Initiative
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY
U.S. DEPARTMENT OF HOMELAND SECURITY
ISE
NATIONAL SHERIFFS' ASSOCIATION
SHERIFFS' ASSOCIATION
MAJOR COUNTY
ESTABLISHED 1998
MAJOR CITIES CHIEFS POLICE ASSOCIATION
1
ESTABLISHED 1949
INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE
IACP
POLICE
SINCE 1893
CRIME STOPPERS U·S·A
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

If You See Something, Say Something™ Campaign Overview

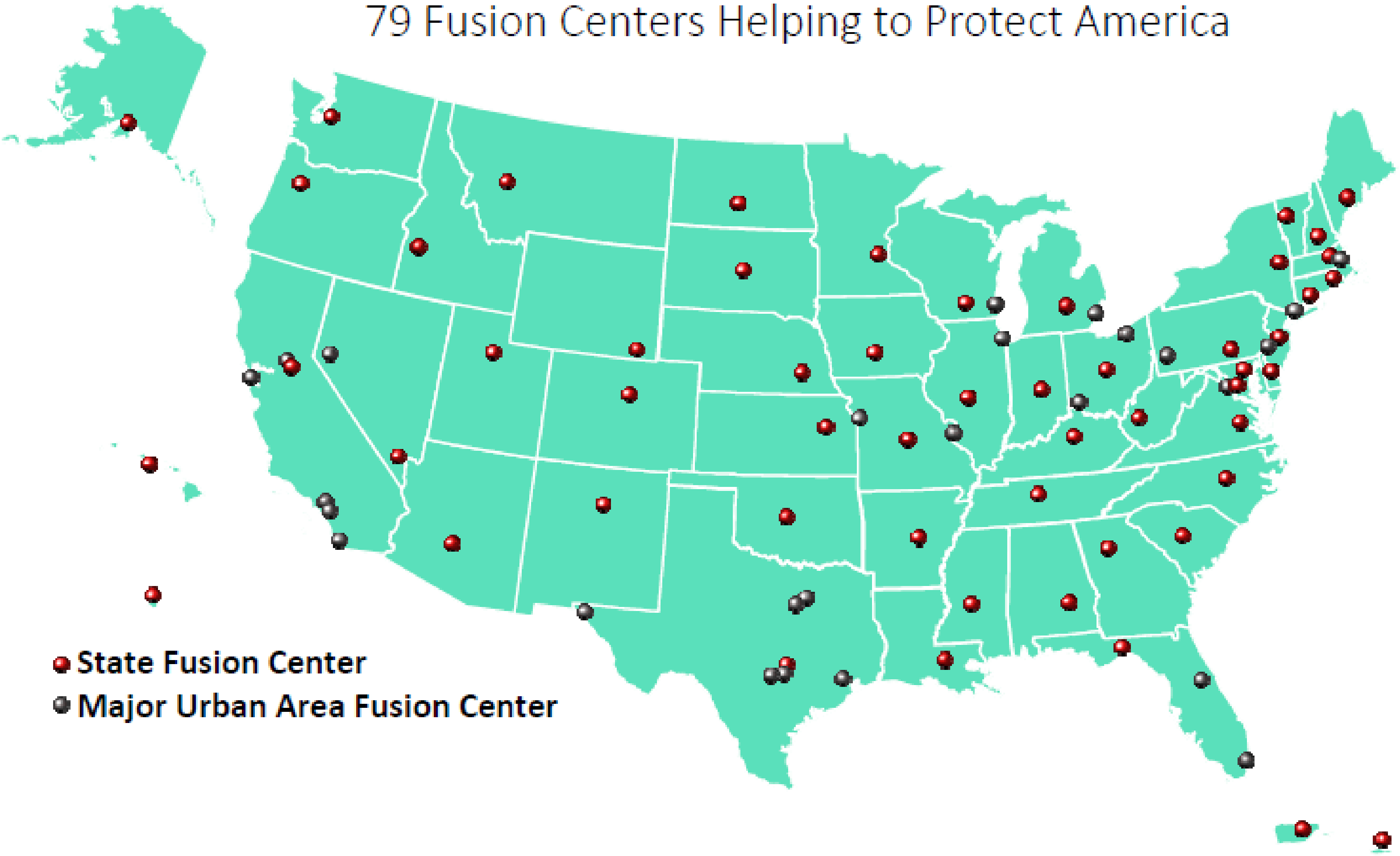
- Launched in 2010
- Simple and effective program to raise public awareness of indicators of terrorism and terrorism-related crime
- Emphasizes the importance of reporting suspicious activity to the proper state and local law enforcement authorities


if you
SEE
something
SAY
something™
If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

The "If You See Something, Say Something™" campaign to raise public awareness of indicators of terrorism and terrorism-related crime can be viewed at: http://www.dhs.gov/if-you-see-something-say-something-campaign.

Fusion Centers

The National Network of Fusion Centers (NNFCs)



79 Fusion Centers Helping to Protect America

Role of Fusion Centers

- Receive threat information from the federal government
- Analyzes federal information in the context of local environment and disseminates that information to local, state, and tribal agencies
- Gathers tips, leads, and suspicious activity reports (SARs) from state, local and tribal agencies as well as the public
- Protects the civil liberties and privacy interests of citizens throughout the intelligence process
- Fusion Centers provide the federal government with critical state, local, and tribal information as well as subject matter expertise.

What is the NSI

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners.

The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country and also serves as the unified focal point for sharing SAR information.

Nationwide SAR Initiative (NSI)

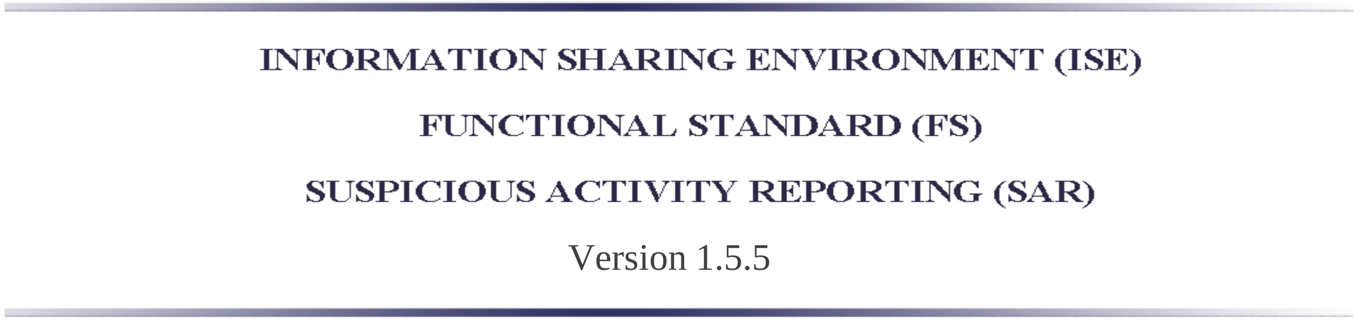
- Focuses on behavior
- Processes the information to identify terrorism-related SARs
- Links these SARs with information from across the nation
- Results in a national effort to detect, prevent, and disrupt terrorism-related activities
  - Using the framework of the ISE-SAR Functional Standard
  - Appropriately protecting privacy/civil rights/civil liberties

NSI Refresh

Widening the aperture.

- *Counterterrorism*
- Mass Casualty Events and School Violence
- Transnational Organized Crime
- Cyber Security
- Counterintelligence
- Economic Security

ISE-SAR Functional Standard

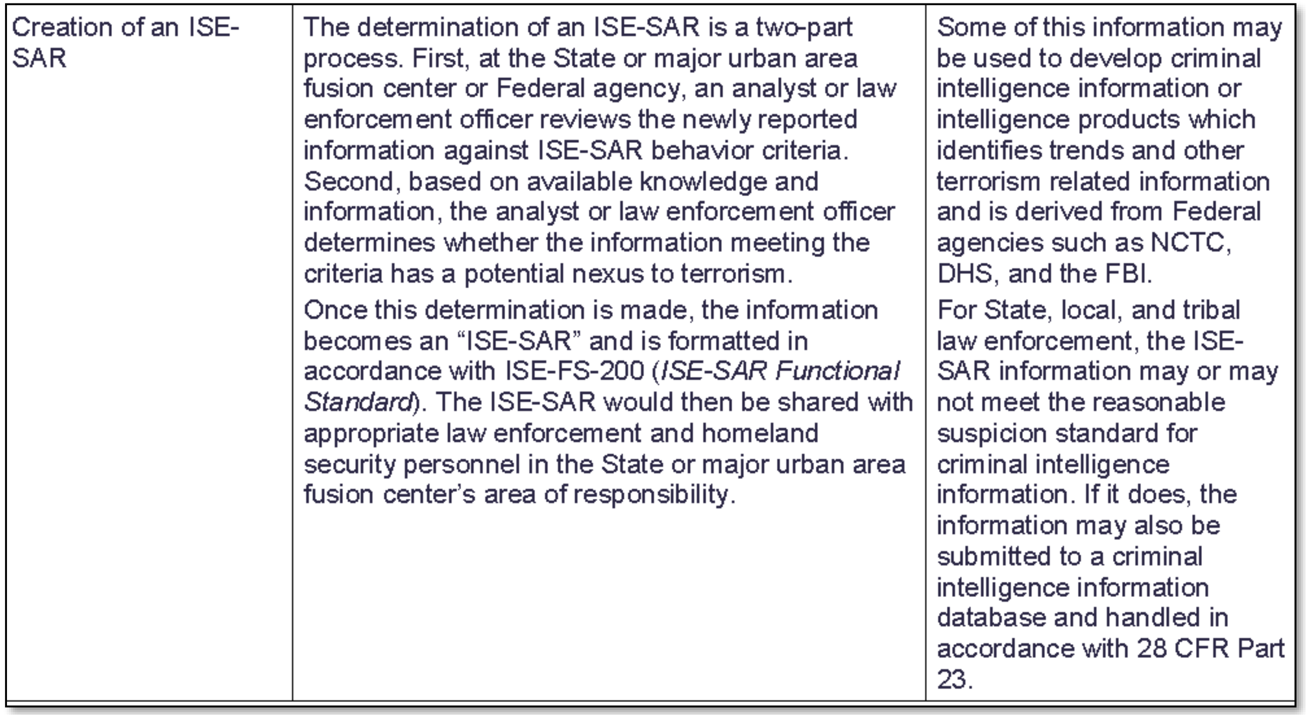


INFORMATION SHARING ENVIRONMENT (ISE)

FUNCTIONAL STANDARD (FS)

SUSPICIOUS ACTIVITY REPORTING (SAR)

Version 1.5.5

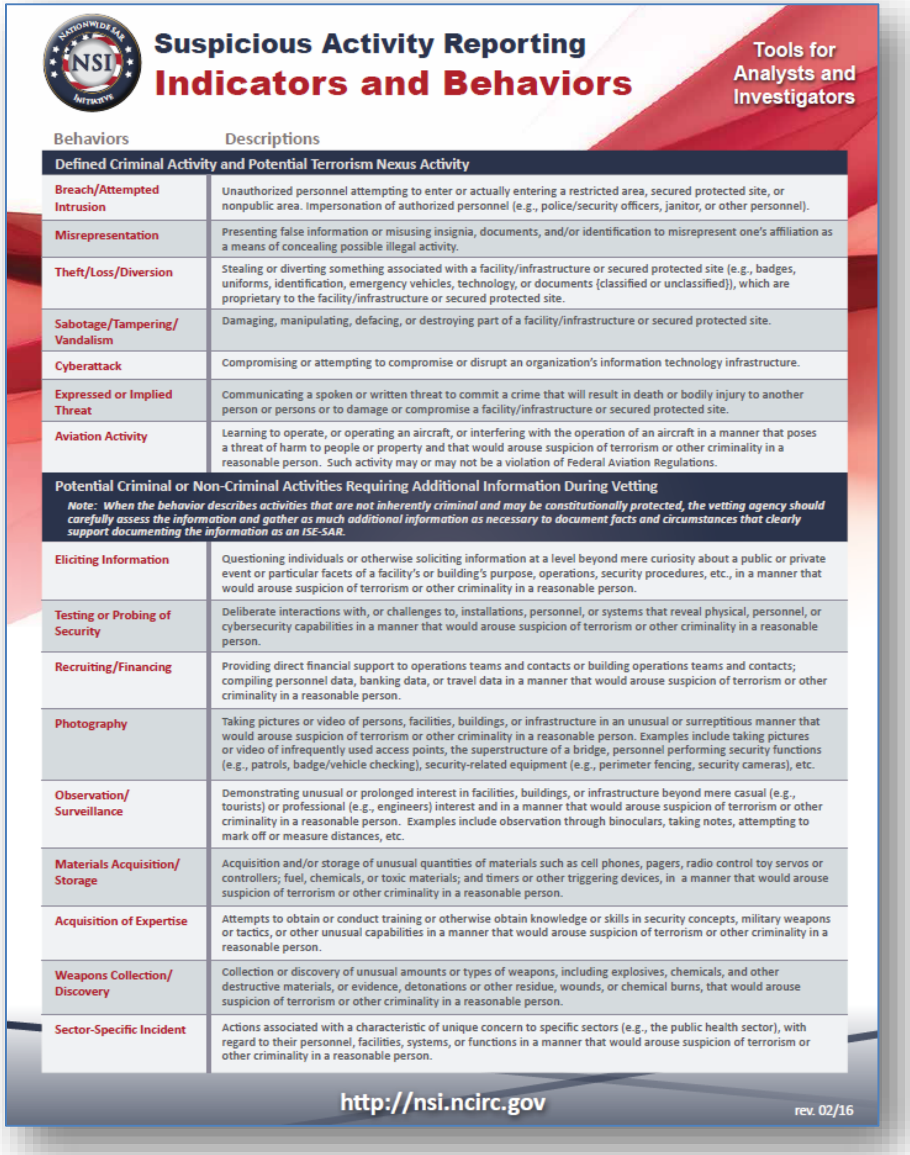


Creation of an ISE-SAR	The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential nexus to terrorism. Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (*ISE-SAR Functional Standard*). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.	Some of this information may be used to develop criminal intelligence information or intelligence products which identifies trends and other terrorism related information and is derived from Federal agencies such as NCTC, DHS, and the FBI. For State, local, and tribal law enforcement, the ISE-SAR information may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23.

NSI Process

SAR Behaviors

- Vetting and Submission
  - Information submitted by law enforcement is reviewed by a trained analyst against the NSI Vetting Guidelines
  - Functional Standard-compliant information is either shared in the NSI SDR or reported in eGuardian
  - Only the information determined by the submitting agency as shareable is available for search/view



Suspicious Activity Reporting Indicators and Behaviors

Tools for Analysts and Investigators

Behaviors	Descriptions
Defined Criminal Activity and Potential Terrorism Nexus Activity	
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.
Sabotage/Tampering/ Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.
Potential Criminal or Non-Criminal Activities Requiring Additional Information During Vetting *Note: When the behavior describes activities that are not inherently criminal and may be constitutionally protected, the vetting agency should carefully assess the information and gather as much additional information as necessary to document facts and circumstances that clearly support documenting the information as an ISE-SAR.*	
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.
Observation/ Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials Acquisition/ Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Weapons Collection/ Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.

http://nsi.ncirc.gov

rev. 02/16

Definitions of SAR and ISE SAR

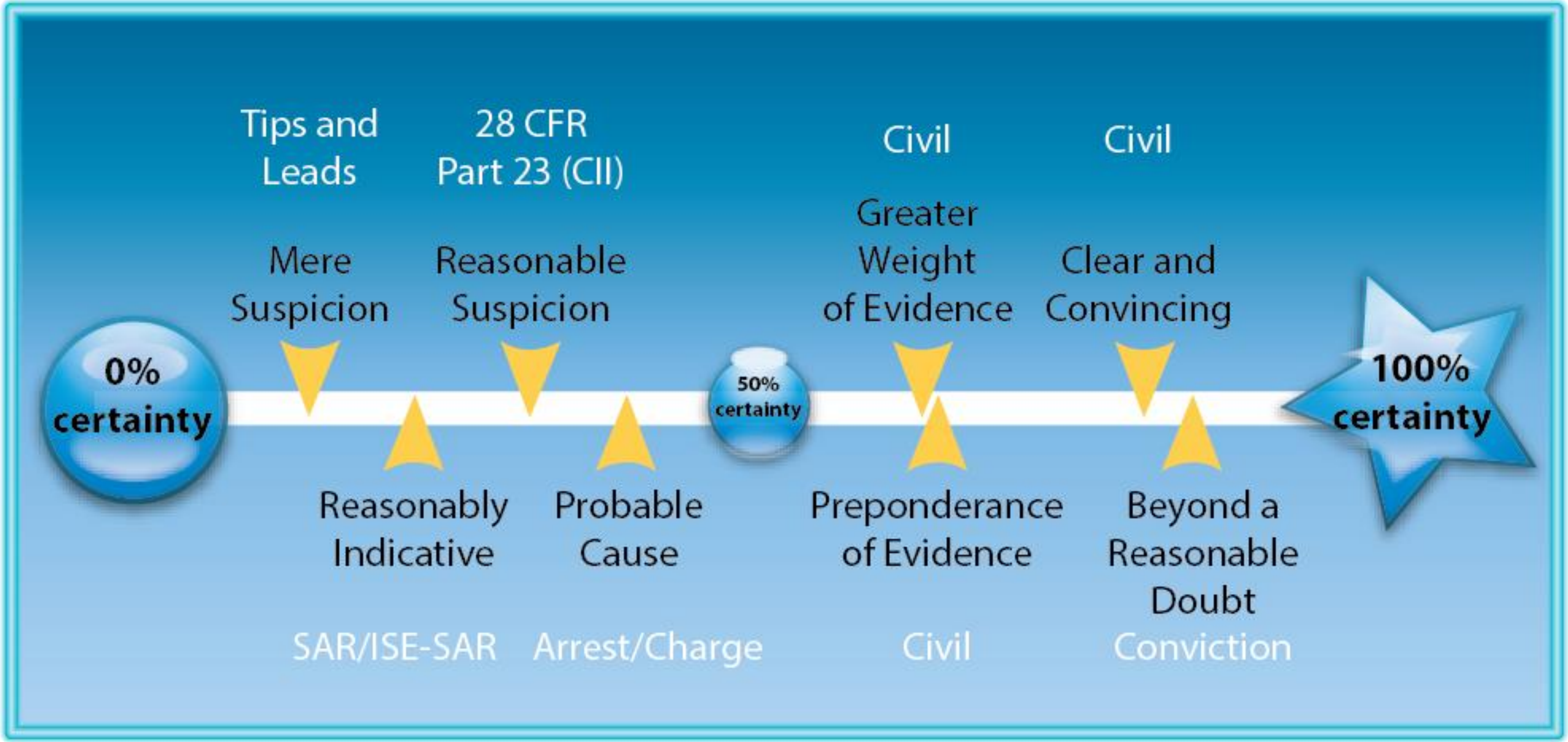
- **Suspicious Activity Report (SAR):** Official documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity

- **ISE-Suspicious Activity Report (ISE-SAR):** An ISE-SAR is a SAR that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE
  - *the term "other criminal activity" must refer to criminal activity associated with terrorism and must fall within the scope of the 16 terrorism pre-operational behaviors identified in the Functional Standard.*

Reasonably Indicative

- Reasonably Indicative Operational Concept
  - Reasonably indicative is a concept for documenting and sharing a suspicious activity report that takes into account the circumstances in which that observation is made which creates in the mind of the reasonable observer, including a law enforcement officer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases where an officer is the observer or documenter of the observed behavior reported to a law enforcement agency

Progression of Information Development



ISE-SAR Criteria Guidance

- Defined Criminal Activity and Potential Terrorist Nexus Activity
  - Breach/Attempted Intrusion
  - Misrepresentation
  - Theft/Loss/Diversion
  - Sabotage/Tampering/Vandalism
  - Cyberattack
  - Expressed or Implied Threat
  - Aviation Activity

ISE-SAR Criteria Guidance

- Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During Investigation
  - Eliciting Information
  - Testing or Probing of Security
  - Recruiting/Financing
  - Photography
  - Observation/Surveillance
  - Materials Acquisition/Storage
  - Acquisition of Expertise
  - Weapons Collection/Discovery
  - Sector-Specific Incident

Vetting Issues

- Each jurisdiction must follow its own policies, regulations, and/or laws regarding the initial timeline for vetting, follow-up reviews, and updates to SAR information
- Follow your fusion center's SAR standard operating procedure and agency privacy policy regarding the submission of SAR information that may not meet the Functional Standard
- Vetting is based on analyst/investigator training and experience and must be viewed in the context, facts, and circumstances of the incident

Vetting Issues

- Analysts or investigators who need additional information for SARs are encouraged to follow up with the submitting agency
- Not all information is reasonably indicative of terrorism or criminal activity
  - When the behavior describes activities that are not inherently criminal and may be constitutionally protected, the vetting agency should carefully assess the information and gather as much additional information as necessary to document facts and circumstances that clearly support documenting the information as an ISE-SAR

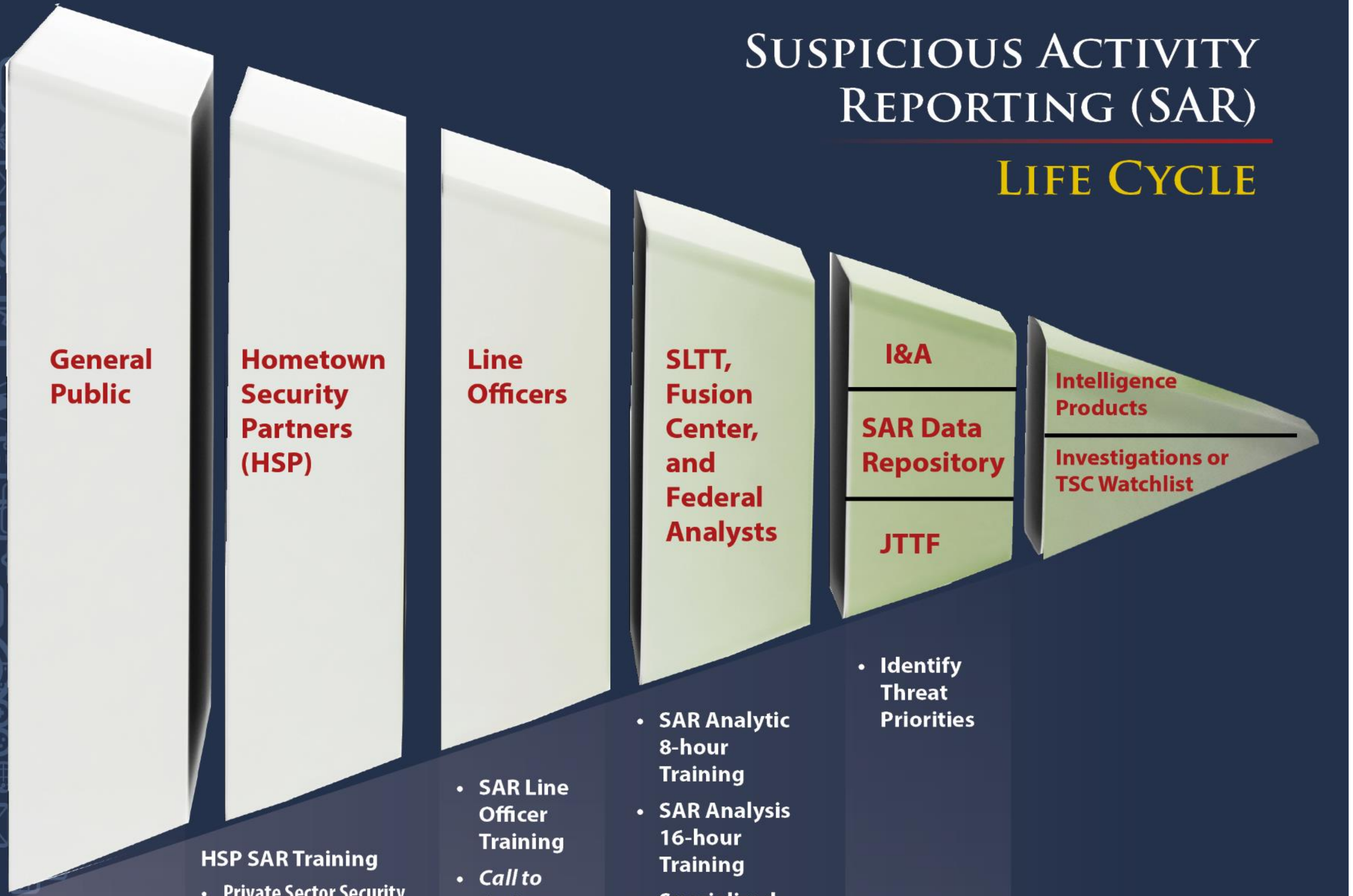
Submission

- Information submitted by law enforcement is reviewed by a trained analyst/investigator against the NSI ISE-SAR vetting guidance
- Context, facts, and circumstances should be used to interpret the behaviors
- Functional Standard-compliant information is either shared in the NSI SDR or reported in eGuardian
  - Only the information determined by the submitting agency as shareable is available for search/view

MILLIONS OF TIPS AND LEADS → THOUSANDS OF SARs → HUNDREDS OF INVESTIGATIONS

SUSPICIOUS ACTIVITY REPORTING (SAR)

LIFE CYCLE



General Public

Hometown Security Partners (HSP)

Line Officers

SLTT, Fusion Center, and Federal Analysts

I&A

SAR Data Repository

JTTF

Intelligence Products

Investigations or TSC Watchlist

if you SEE something SAY something™

HOW THE NSI SUPPORTS THESE EFFORTS

- Building Community Partnerships
- If You See Something Say Something™

HSP SAR Training

- Private Sector Security
- Fire and EMS
- Probation, Parole, and Corrections
- Public Safety Telecommunications
- Emergency Management
- Maritime Sector
- Public Health and Health Care Partners

- SAR Line Officer Training
- *Call to Action: Unified Message*
- State and Local Anti-Terrorism Training (SLATT®)

- SAR Analytic 8-hour Training
- SAR Analysis 16-hour Training
- Specialized Analytic Seminar Series

- Identify Threat Priorities

UNCLASS

Privacy Considerations

Privacy, Civil Rights, and Civil Liberties Considerations for the Suspicious Activity Reporting (SAR) Vetting Process

P/CRCL Issues: How Do They Arise?

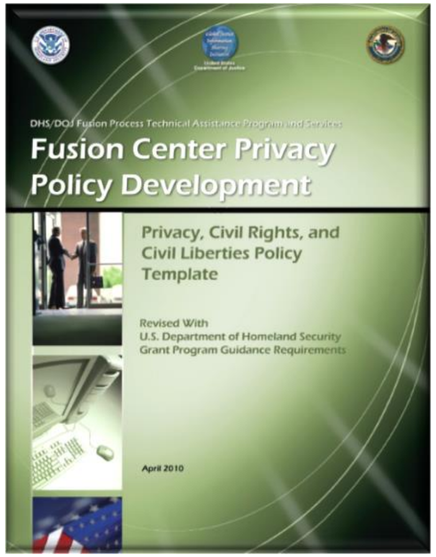
- Initial collection was illegal or inappropriate
- Poor data quality
  - Sharing of erroneous or otherwise deficient data may lead to denial of benefit or liberty
- Data used for purpose other than original purpose
- Mishandling/misuse of records
- Inappropriate storage, dissemination, and retention
- Data breach
- Lack of redress available to the individual

P/CRCL Issues: What Is the Harm?

- To individual
  - Personal harm (job, reputation)
  - Loss of benefits or liberties
- To agency
  - Limitation/loss of sources, methods, and information
  - Disciplinary action and job loss
  - Limitation/shutdown of operation and court action
  - Economic harm
  - Loss of public trust

P/CRCL Issues: What are the Solutions?

- Comprehensive privacy and civil liberties protection policies (e.g., fusion center privacy policies)
- Enhanced P/CRCL protections
  - Information systems
  - Technology
- Transparency and accountability
- Privacy Impact Assessments
- Community outreach
- Training, technical assistance, national standards


DHS/DOJ Fusion Process Technical Assistance Program and Services

Fusion Center Privacy Policy Development

Privacy, Civil Rights, and Civil Liberties Policy Template

Revised With
U.S. Department of Homeland Security
Grant Program Guidance Requirements

April 2010

Training and Outreach Resources

Suspicious Activity Reporting
Explosive Precursors Point of Sale Training

Domestic and international terrorism plots did not end with 9/11—in fact, they continue to grow and threaten the United States, its citizens, and its critical infrastructure.

Reporting suspicious activity to law enforcement provides leads to further investigations and helps prevent crime, including terrorism.

In the course of their daily duties and responsibilities, retail professionals may observe suspicious activity that could be an indicator of a terrorist attack or other criminal activity. This online training video was developed to assist retail professionals at the point of sale for explosive precursors in:

- Recognizing what kinds of suspicious behaviors are associated with pre-incident terrorism activities.
- Understanding how and where to report suspicious activity.
- Protecting privacy, civil rights, and civil liberties when reporting or documenting information.

Point-of-sale retail professionals can incorporate this video into their training programs for current or newly hired personnel.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

This training was developed by the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), a partnership of agencies at all levels that provides law enforcement with another tool to combat crime and terrorism. The NSI has established a national capacity for gathering, documenting, processing, analyzing, and sharing terrorism-related SARs. Visit the NSI website at http://nsi.ncirc.gov for resources to assist agencies in developing and increasing the effectiveness of their SAR processes and counterterrorism activities.

Hometown Security Partners

The Suspicious Activity Reporting Explosive Precursors Point of Sale Training is one in a series of trainings developed by the NSI. In addition to providing training for the law enforcement community, the NSI has developed this SAR awareness training for partners with similar missions, or "hometown security partners."

These partners include:

- Retail professionals at the point of sale for explosive precursors
- Emergency management professionals
- Private sector security officers and personnel and those charged with protecting the nation's critical infrastructure
- Probation, parole, and corrections professionals
- Public safety telecommunications professionals (e.g., 9-1-1 operators)
- Fire and emergency medical services professionals
- Maritime industry professionals
- Public health and health care partners

Training Available at No Cost

The Suspicious Activity Reporting Explosive Precursors Point of Sale Training is provided at no cost to retail professionals.

To Access the Online Training

Access the training through the NSI website at:

http://nsi.ncirc.gov/hsptregistration/explosive_precursors/

For More Information

E-mail nsiinformation@ncirc.gov.

Rev. 06/17

Resources

To view/download class information as well as intelligence resources

Visit https://filecloud.iir.com/X/DHS2018

Password - 2018DHS

NSI Public Web Site

https://nsi.ncirc.gov

Questions

Wesley Moy, Ph.D.

nsiinformation@ncirc.gov