Suspicious Activity Reporting (SAR)
Line Officer Training

Domestic and international terrorism plots did not end with 9/11—in fact, they continue to increase and threaten the United States, its citizens, and its critical infrastructure. The Suspicious Activity Reporting (SAR) Line Officer Training focuses on the critical role frontline law enforcement officers have in the effective implementation of the SAR process by identifying and documenting suspicious activity.

This online training video was developed to assist law enforcement officers and support personnel in:

- **Recognizing what kinds of suspicious behaviors** may be related to pre-incident terrorism activities.
- **Understanding how to document and report suspicious activity.**
- **Protecting privacy, civil rights, and civil liberties** when reporting or documenting information.

This training also provides information about integrating the Nationwide SAR Initiative (NSI) into your organization's operations. Behaviors and indicators outlined in the ISE-SAR Functional Standard are covered in the training, along with scenarios relating to suspicious activity reporting.

Law enforcement agencies can incorporate this video into their roll-call briefings and training programs for current or newly hired personnel.

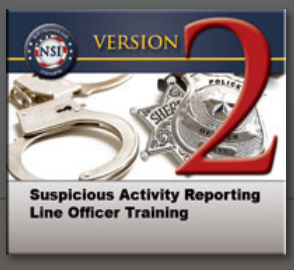
Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

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.

Training Available at No Cost

The SAR Line Officer Training is provided at no cost to law enforcement personnel.

To Access the Online Training



Access the training through the NSI website at:

https://nsi.ncirc.gov/sarlotregistration/version2/

For More Information

Email nsiinformation@ncirc.gov.

Rev. 01/18

Suspicious Activity Reporting
Indicators and Behaviors

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.