SUSPICIOUS ACTIVITY REPORTING

Information for Officers Reporting on Suspicious Activity

When completing a suspicious activity report (SAR), officers must remember the following:

1. The information for the SAR must be legally obtained.
2. The information submitted must be relevant to the identification of the subject or the subject's criminal conduct or activity.
3. The information gathered cannot be based solely on the political, religious, or social views, associations, or activities of any individual or any group.

What if I am dispatched to a call for police service and then once on scene discover SAR-related activity?

Handle the call as usual, including all reports that your agency requires. If you observe SAR activity not directly related to a reportable crime, please complete a separate report with the SAR information.

What information should I include when documenting a suspicious activity?

"Everything you can!"

It is important to include all information obtained so that the full context of the incident is apparent to anyone who reviews the report. This includes detailed descriptions of people, vehicles, facilities, etc. It is also important to include a complainant's information (name, phone number, etc.) if available.

The Nationwide SAR Initiative (NSI) is 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 SARs.

A suspicious activity report (SAR) is used to document any reported or observed activity or any criminal act or attempted criminal act that an officer believes may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may be the result of observations or investigations by police officers or may be reported to them by private parties.

For more information: **http://nsi.ncirc.gov**

BJA Bureau of Justice Assistance
U.S. Department of Justice

This project was supported by Grant No. 2008-DD-BX-K520 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Issued 09/10

Suspicious Activity Reporting
Indicators and Behaviors

Behaviors	Descriptions
Potential Criminal or Noncriminal Activities Requiring Additional Information During Investigation	
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 of Security	Interactions with or challenges to installations, personnel, or systems that reveal physical personnel or cybersecurity capabilities.
Recruiting	Building 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. All reporting on photography should be done within the totality of the circumstances.
Observation/ Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition of unusual quantities of precursor materials such as cell phones, pagers, fuel, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts (military weapons or tactics) or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector) with regard to their personnel, facilities, systems, or functions.
Defined Criminal Activity and Potential Terrorism Nexus Activity	
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter 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.
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 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. May or may not be in violation of Federal Aviation Regulations.