Safeguarding America—It All Starts With You

10 Ways to Integrate Suspicious Activity Reporting Into Your Agency's Operations

Observing suspicious activity and taking appropriate action can solve crimes and save lives. Often, crimes begin at the local level. By maximizing information from citizens, law enforcement, and public safety officials; employing intelligence-led policing; and collaborating with fusion centers and appropriate partners, agencies can use actionable information and intelligence to effectively and efficiently detect and deter criminal acts. Your part in the process is vital to our nation's information sharing environment.

A report entitled *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* was developed to describe the all-crimes approach to gathering, processing, reporting, analyzing, and sharing suspicious activity by local law enforcement agencies. The report and its recommendations (including the continued emphasis on the protection of privacy and civil liberties) are important for establishing national guidelines that will allow for the timely sharing of SAR information. Although every jurisdiction will develop policies and procedures that take into account the unique circumstances and relationship with its community, below are some strategies your agency can use to integrate the SAR process into its operations.

Suspicious activity is described as "observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity."

1. **RECOGNIZE** the importance of suspicious activity reporting (SAR), understand your role in the SAR process, and know that your involvement makes a difference. Strong leadership is an essential element. Gain support from personnel, leadership, and policymakers both internally and externally.

2. **DEVELOP** a data collection process and a secure standardized reporting format for sharing suspicious activity. Review other agencies' SAR process missions/Standard Operating Procedures (SOPs) to better understand the process and identify promising practices. Define and communicate trends in terrorism-related activity, geographically specific threat reporting, dangers to critical infrastructure, and general situational awareness.

3. **LEVERAGE** and adopt the use of common national standards to enhance the capability to quickly and accurately analyze suspicious activity data, such as the Information Sharing Environment (ISE) Functional Standard (FS) for Suspicious Activity Reporting, the National Information Exchange Model (NIEM), and the records management system (RMS) and computer-aided dispatch (CAD) functional standards.

4. **INCORPORATE** appropriate guidelines and concepts into your operations, such as intelligence-led policing, the *National Criminal Intelligence Sharing Plan*, the *Fusion Center Guidelines*, the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*, and privacy and civil liberties templates. Use these guidelines to establish and integrate the SAR process.

5. **IMPLEMENT** and adhere to your agency's privacy policy, and ensure that the privacy, civil rights, and civil liberties of citizens are protected. Evaluate your privacy policy and update it, if necessary, to ensure that gathering, documenting, processing, and sharing information regarding terrorism-related criminal activity are specifically addressed. Ensure that the privacy policy is transparent, and communicate the policy to the public and stakeholders.

6. **TRAIN** all agency personnel on the SAR process and institutionalize it within your agency. Ensure that law enforcement and public safety personnel understand the SAR process and what internal policies or protocols exist to share appropriate information. Learn about available training to increase or enhance abilities, such as the Nationwide SAR Initiative (NSI) training programs, available at https://www.dhs.gov/nsi, or the State and Local Anti-Terrorism Training (SLATT®) Program, available at www.SLATT.org.

7. **INSTITUTIONALIZE** the gathering of suspicious activity information at the street level, and standardize the reporting of such data so that it may be shared with other appropriate public safety partners, such as your criminal intelligence unit, the state or regional fusion center, the Joint Terrorism Task Force (JTTF), and other law enforcement and public safety partners, as appropriate. Once your agency's SAR process is developed, continuous improvements will ensure the integrity and institutionalization of the process within the agency.

8. **EDUCATE** citizens, businesses, and partners on suspicious activity reporting and how to report activity to the appropriate officials. Consider participating in the Building Community Partnerships (BCP) initiative, which was established to assist fusion centers and law enforcement agencies in engaging with and developing productive relationships with the critical sector and community stakeholders they serve to enable partnerships in the protection of critical infrastructure and the prevention of crime and terrorism. Additional information on the BCP initiative is available at https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training. Develop outreach materials to educate the public on recognizing and reporting behaviors and incidents indicative of terrorism or other criminal activity. In addition, existing SAR awareness training programs, such as the NSI's Hometown Security Partners Training modules, available at https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training can be leveraged to educate those partners with similar missions to law enforcement.

9. **PARTNER** with other law enforcement, public safety, private sector, and state or major urban area fusion centers. Foster interagency collaborations to maximize each other's resources and create an effective and efficient information sharing environment.

10. **CONNECT** to a major information sharing network, such as the Regional Information Sharing Systems® Secure Cloud (RISSNET™), the Federal Bureau of Investigation's Law Enforcement Enterprise Portal (LEEP), or the U.S. Department of Homeland Security's Homeland Security Information Network (HSIN). Leverage proven and trusted technology to share information, communicate, and access additional resources.

FOR MORE INFORMATION

To contact the National Threat Evaluation and Reporting (NTER) Office, NSI program management team, email: **NTER@hq.dhs.gov**
Website: **https://www.dhs.gov/nsi**

This project was supported by Grant No. 2011-DG-BX-K003 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Homeland Security (DHS) and the Nationwide Suspicious Activity Reporting 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.