Suspicuous Activity Reporting

Process Implementation Checklist

A companion document to the Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project report
The Suspicious Activity Reporting (SAR) process focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime and establishing a process to share information to detect and prevent criminal activity, including crime associated with domestic and international terrorism. Implementation of the SAR process can be accomplished within the agency’s existing framework to gather, document, process, analyze, and share behaviors and events that are indicative of criminal activity.

After the horrific events of September 11, 2001, agencies at all levels of government recognized the risks that can result from not sharing information, as well as the value and benefits of sharing critical information—"connecting the dots." The National Strategy for Information Sharing (NSIS) was subsequently developed to establish, in part, a nationwide vision for the sharing of suspicious activity. One of the tasks for the federal government, as identified in the NSIS, is to “establish a unified process to support the reporting, tracking, processing, storage, and retrieval” of Suspicious Activity Reports.

A Suspicious Activity Report (SAR) is defined as “official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.”

In an effort to implement the tenets of the NSIS, local, state, tribal, and federal agencies have partnered to develop a nationwide SAR capability. To meet these requirements, an end-to-end process—the gathering, processing, reporting, analyzing, and sharing of suspicious activity—was adopted by major national law enforcement organizations. This process, also referred to as the SAR process, is graphically depicted on pages 4 and 5. A key goal of this process is ensuring that behavior which
may be indicative of terrorist activity is shared with fusion centers and Joint Terrorism Task Forces (JTTF) in an expedited manner so that broad partnership resources can be leveraged as quickly as possible.

All agencies, regardless of size or jurisdiction, have a role in the nationwide SAR process. It is essential that local, state, tribal, and federal agencies work together to share SAR information in order to prevent and deter another terrorist attack on American soil.

Using this checklist in developing an internal SAR process will aid agencies in their crime prevention efforts and assist with successfully incorporating local, state, and tribal agencies into the nationwide SAR process.

For each checklist step and associated “action items,” refer to the Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project for additional guidance and recommendations for implementation.

Included at the end of the checklist is an overview of the Information Sharing Environment (ISE) Shared Spaces concept—which is a solution to sharing SAR data among local, state, tribal, and federal agencies—as well as a listing of benefits for participating in the nationwide SAR process.
Federal agencies produce and make available intelligence and other information products to support the development of geographic risk assessments by state and major urban area fusion centers.

National coordinated information needs on annual and ad hoc basis

Authorized ISE participants access and retrieve ISE-SAR

ISE-SAR posted in ISE Shared Spaces

State and major urban area fusion centers, in coordination with local or federal officials, develop information requirements based on risk assessment

State and major urban area fusion centers, in coordination with local or federal officials, develop risk assessments

As shown in the diagram below, certain steps—highlighted in red—in the SAR process focus on the activities of local, state, and tribal agencies. By following these steps, agencies can be assured that their SAR activities are in alignment with and can support crucial information sharing. This diagram will also help identify gaps in an agency's current process that may need to be addressed and/or corrected.
Frontline law enforcement personnel (federal, state, local, and tribal) are trained to recognize behavior and incidents that may indicate criminal activity associated with terrorism. Community outreach plan implemented.

Suspicious Activity Processing Steps

- Planning
- Gathering and Processing
- Analysis and Production
- Dissemination
- Reevaluation

Observation and reporting of behaviors and incidents by trained law enforcement personnel during their routine activity.

Supervisory review of the report in accordance with departmental policy.

In major cities, SAR reviewed by trained counterterrorism expert.

SAR made available to fusion center and/or JTTF.

At fusion center or JTTF, a trained analyst or law enforcement officer determines—based on information available, knowledge, experience, and personal judgment—whether the information meeting the ISE-SAR criteria may have a terrorism nexus.
The chief executive and agency leadership must recognize the importance of implementing a SAR process within their agency and champion the efforts of the SAR process and the Nationwide SAR Initiative (NSI) both inside and outside the agency.

**Action Items**

- Closely collaborate with partners such as fusion centers, homeland security officials, JTTFs, and the eGuardian program.
- Brief command staff/senior management on the SAR implementation process, to include policy development, privacy and civil liberties protections, technology, training, and community outreach.
- Assign primary responsibility for implementing the SAR process to a command-level position.
- Provide training to command staff/senior management on the implementation of the SAR process using agency training or programs already developed.
Examine the agency’s business process to identify current SAR processes in place, and determine what processes to develop and/or enhance. Once complete, develop an order/Standard Operating Procedures (SOPs) directing the gathering, processing, reporting, analyzing, and sharing of suspicious activity. Leverage the use of national standards, and incorporate national guidelines into the business process and agency SOPs.

**Action Items**

- Review other agencies’ SAR process mission/SOPs to better understand the process and to identify promising practices to assist in the development of your own agency policy and mission statement.

- Simplify the reporting process by modifying agencies’ current reports—basic incident report, offense report, information report, or field interview report—to include fields to capture SAR data (consider using one report as the primary intake for standardization).

- Identify and establish intake points for the collection and receipt of SARs (one centralized location).

- Develop an electronic means or modify your current system (i.e., records management system [RMS]) to gather, process, report, analyze, and share SAR data within your agency in real time.
INTEGRATE NATIONAL GUIDELINES INTO STANDARD OPERATING PROCEDURES

- Adopt the standardized behavioral-specific codes used to identify SARs, located in the Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR).
- Define a process for forwarding data to the urban area, regional, or statewide fusion center and JTTF.
- Ensure that SARs receive an initial vetting within 24 hours of being reported.
- Develop a method for determining disposition of SAR data (e.g., whether to respond, refer, determine unfound, or take other action).
- Develop a system where SAR data is retrievable.
- Develop a mechanism for providing timely feedback to the original submitter of the SAR information.
Develop and/or enhance and **implement** the agency privacy policy to ensure that privacy and civil liberties are protected when performing all steps of the SAR process.

**ACTION ITEMS**

- Use legal/privacy advisors when developing the agency’s privacy and civil liberties protection policy.

- Promulgate the SAR privacy policy agencywide to stress the importance of privacy, civil rights, and civil liberties protections during the SAR process and within the agency.

- The privacy policy should be transparent and communicated with the public, community organizations, and other groups as appropriate.
Training is a vital component of an agency’s SAR process implementation. Personnel at all levels should receive training on the SAR process to ensure that it is institutionalized within the agency.

**Action Items**

- Develop a framework and timetable for training all personnel within the agency.

- Training should focus on:
  
  - The importance of privacy and civil liberties protections.
  
  - The **gathering** of suspicious activity through behavior-based policing.
    
      - Behavior-based policing includes behaviors and/or incidents known to be exhibited by terrorists that would be collected in a terrorism-related Suspicious Activity Report.
  
  - The mechanism for **reporting** suspicious activity (standardization).
  
  - The **processing** of SARs within the agency.
  
  - The steps in **analyzing** the SAR data.
  
  - The appropriate **sharing** of suspicious activity within and outside the agency.

- Implement an evaluation program for modifying and enhancing the SAR training program based on emerging trends, lessons learned, and identified gaps.
Once an agency’s SAR process is developed, continuous improvements will ensure the integrity and institutionalization of the process within the agency. Criminals are continually modifying their methods, and law enforcement operations must also continue to adapt to meet these changes.

**Action Items**

- Develop a liaison officer program to ensure that terrorism-related suspicious activity is being gathered and reported to the proper personnel, local JTTF, and fusion center.

- Conduct periodic audits on SAR data by command-level staff or designees.

- Develop qualitative and quantitative measures on the SAR process to gauge effectiveness (management accountability reports).

- Modify the agency SAR process based on Priority Information Needs (PINs) for emerging trends/behaviors.

- Incorporate the SAR process into the development of alerts, warnings, notifications, and other relevant reports for critical infrastructure/key resources.
Educate the community on the SAR process to ensure transparency and openness and to elicit their support.

**Action Items**

- Provide educational outreach to the public regarding the SAR process and policies through initiatives such as:
  - Internet-based newsletters
  - E-mail notifications to stakeholders
  - Media commercials
  - Officer-to-citizen interaction programs
  - Distribution of CDs and DVDs related to the reporting of suspicious activity
  - Community awareness training
  - Informational flyers
Partner with other law enforcement agencies, public safety, public health, and external stakeholders. Connect to nationwide law enforcement information sharing networks.

**Action Items**

- Inform external stakeholders (mayor, city council, legislature, etc.) on the SAR process to gain their support.
- Provide educational outreach and develop partnerships with public safety (fire, emergency management services, health agencies, etc.) and the private sector (financial institutions, private security, power plants, etc.) regarding the SAR process.
- Become a member of a secure law enforcement network, such as RISSNET™, Law Enforcement Online (LEO), or the Homeland Security Information Network (HSIN).
- Access the state’s criminal justice network (if available).
- Access the state or regional intelligence database (if available).
- Access the state or regional fusion center (if available).
- Ensure that the agency has the ability to send and receive secure e-mail.
- Develop the ability to export RMS data in the National Information Exchange Model (NIEM) Extensible Markup Language (XML) format for SARs.
- Continue to collaborate with nationwide partners such as fusion centers, homeland security officials, JTTFs, and the eGuardian program.
The ISE Shared Spaces concept is a networked data and information repository used to make standardized terrorism-related information available through Common Terrorism Information Sharing Standards applications and services.

Developing a SAR process and involvement in the ISE Shared Spaces will provide agencies with the ability to access local, regional, state, tribal, and federal SAR data. ISE Shared Spaces provide an easy solution for agencies to share terrorism-related suspicious activity information, while still maintaining control of their data.

Law enforcement agencies are able to share their information with other agencies without directly accessing each other’s internal databases. Each agency has control of the information it makes available for sharing; this is accomplished by each agency’s exporting to its external server all information that it is willing to share with other agencies. These external servers are then made available for search only by authorized user agencies via a secure network. There are multiple examples of ISE Shared Spaces, including servers owned and operated by local jurisdictions, eGuardian, and the U.S. Department of Homeland Security (DHS).
User’s Secure Network
RISSNET / LEO / HSIN Intel

www.ncirc.gov
Entry point into the ISE Shared Spaces Environment

ISE-SAR
SHARED SPACES
Benefits of Establishing or Enhancing a SAR Process

Using the SAR Process, Agencies Can:

- Benefit from the ability to access other jurisdictions’ information to assist them with their local efforts in identifying and preventing criminal activity related to terrorism.
- Utilize the SAR process to assist in the development of intelligence-led policing models.
- Apply the SAR data to the COMPSTAT process for management accountability and resource allocation.
  - COMPSTAT (COMPuter STATistics) is an accountability process—developed originally by the New York City Police Department and adopted by many law enforcement agencies around the country—that uses crime statistics to drive decision making on the deployment of resources and provides a methodology to measure police activity.
- Apply geospatial visualization of SAR data to assess relationships to critical infrastructure/key resources.
- Enhance analytic capabilities to better identify linkages.
- Enhance analytic capabilities to track SAR activity by date, time, and/or location.
**SAR Initiative Resources**

*National Strategy for Information Sharing*

*Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*

*Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)*
http://www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued.pdf

*National Information Exchange Model*
www.niem.gov

*Additional resources and publications on the SAR initiative or the SAR process can be located at:*
www.ncirc.gov
www.ise.gov
This project was supported by Grant No. 2008-DD-BX-K480 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

Special thanks to the leadership of the Los Angeles, California, Police Department for their initiative and guidance in the creation of this document.

Acknowledgement is also provided to the SAR initiative partners: Major Cities Chiefs Association (MCCA); U.S. Department of Justice’s Global Justice Information Sharing Initiative Criminal Intelligence Coordinating Council; International Association of Chiefs of Police (IACP); Major County Sheriffs’ Association (MCSA); Bureau of Justice Assistance (BJA); U.S. Department of Homeland Security (DHS); Program Manager, Information Sharing Environment (PM-ISE); Office of the Director of National Intelligence (ODNI); U.S. Department of Defense (DoD); and the FBI eGuardian program.