

Reporting Suspicious Activity – Critical for Terrorism Prevention

Public safety personnel are uniquely positioned in their communities to report activities and behaviors associated with criminality, including activities and behaviors with a nexus to terrorism. Public safety personnel may obtain information from interactions with the public, during calls for service, or while conducting investigations. This publication highlights the importance of public safety awareness of Suspicious Activity Reporting (SAR)³ mechanisms and encourages federal, state, local, tribal, and territorial (FSLTT) law enforcement partners—as well as the Department of Defense (DOD)—to document SAR in their jurisdictions.

- The Nationwide SAR Initiative (NSI) is a joint collaborative effort by DHS, FBI, and SLTT law enforcement partners. It establishes standardized processes and policies that provide the capability for FSLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant SAR through an information-sharing system while protecting individual privacy, civil rights, and civil liberties.
 - eGuardian is the information-sharing system that FSLTT law enforcement agencies, state and local fusion centers, and the DOD use to initiate NSI processes. It provides a global base for SAR in order to facilitate the tracking and management of threats and determine whether particular matters should be closed or opened as predicated investigations. eGuardian also facilitates pattern and trend analysis of SAR information. Information that meets the requirements to be shared is entered into a shared environment known as the Shared Data Repository (SDR)—all law enforcement agencies have the ability to read and add value to incidents in the SDR. Since its inception, eGuardian has expanded to allow the submission of SAR—beyond terrorism—to four other FBI investigative programs: Cyber, Criminal, Weapons of Mass Destruction, and Counterintelligence.

SCOPE: This product is intended for public safety personnel awareness of who, what, when, where, why, and how to report suspicious activity that may be reasonably indicative of criminal activity associated with terrorism and how it plays into the greater CT effort.

“If You See Something, Say Something®”

This DHS campaign is a tool to help raise public awareness of the indicators of terrorism and terrorism-related suspicious activities as well as the importance of reporting suspicious activities to law enforcement authorities.

The campaign's website (www.dhs.gov/seesay) has general materials available for organizations to download, such as:

- State-specific bundles (posters, brochures, graphics, etc.)
- Videos
- Social media toolkits
- Infographics
- Materials translated into 10+ languages

Please contact SeeSay@hq.dhs.gov to learn more, or to become an official campaign partner.

³Information Sharing Environment (ISE) FS SAR 1.5.5 defines a SAR as official documentation of observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.

NOTICE: This is a Joint Counterterrorism Assessment Team (JCAT) publication. JCAT is a collaboration by the NCTC, DHS and FBI to improve information sharing among federal, state, local, tribal, territorial governments and private sector partners, in the interest of enhancing public safety. This product is NOT in response to a specific threat against the United States. It provides general awareness of, considerations for, and additional resources related to terrorist tactics, techniques and procedures, whether domestic or overseas. Consider the enclosed information within existing laws, regulations, authorities, agreements, policies or procedures. For additional information, contact us at JCAT@NCTC.GOV.



NSI CATEGORIES OF INFORMATION THAT MAY BE OBSERVED: The below categories are not exhaustive but are examples of potential reportable activities that may have a nexus to terrorism. The provided examples are fictitious and additional examples can be found on the DHS website under NSI SAR Indicators and Examples.^b

DISCLAIMER: When the behavior describes activities that are not inherently criminal and may be constitutionally protected, public safety personnel 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 information sharing SAR.

- **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. *For example, a military museum received a threatening letter containing a white powder. The letter claimed a full-scale anthrax attack had been launched in retaliation for crimes committed by US Armed Forces.*
- **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. *For example, an individual reported that a former friend and business associate—a chemist—had recently asked him to participate in a terrorist cell operation by providing funding to purchase needed equipment. The funding for the operation was reportedly linked to the illegal production of drugs.*
- **Observation/Surveillance:** Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual interest (e.g., tourists) or professional interest (e.g., engineers) and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, and attempting to mark off or measure distances. *For example, a mall security officer observed a person walking through the mall, filming at waist level and stopping at least twice to film his complete surroundings, floor to ceiling. When the subject was detained, the camera used contained 15 minutes of mall coverage as well as footage of a public train system and photos of a bus.*
- **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, and security procedures in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. *For example, a tour bus company servicing one of the country's national monuments reported that a non-passenger asked a driver many unusual and probing questions about fuel capacity, fueling locations, and fueling frequency that the driver became very concerned about the intent of the questioning.*

^bhttps://www.dhs.gov/sites/default/files/publications/18_0531_NSI_SAR-Indicators-Examples.pdf



SAR Process Implementation Checklist

The following are some recommended steps for agencies who want to create a SAR process within their departments:

- Recognize the importance of implementing a SAR process
- Identify existing SAR processes and determine which still need to be developed
- Incorporate national guidelines into standard operating procedures
- Implement an agency privacy policy
- Train all agency personnel on the SAR process
- Institutionalize the SAR process in the agency
- Educate the community on the SAR process
- Partner with others and connect to information sharing networks^c

IMPROVING SAR FROM THE PUBLIC

Partnerships between public safety personnel and the public can promote enhanced CT awareness and act as a force multiplier for law enforcement. Terrorist disruptions and other mass-casualty incidents offer an opportunity to inform the public on the types of suspicious activity they may observe that are useful to law enforcement and homeland security agencies in detecting and preventing terrorist attacks.

Public safety personnel can use press conferences and media outreach after an incident to emphasize elements of violent extremist mobilization to violence that are observable, and that provide actionable warning of potential attacks or other criminal activity. Explicitly asking the public for help and providing information on what and how to report will encourage increased and informed reporting.

Non-Law Enforcement Critical Partners

While law enforcement partners are key players responsible for SAR reporting, public safety personnel and even private sector security professionals are critical stakeholders for identifying and reporting pre-incident terrorism indicators to prevent acts of terrorism. It is imperative that these non-law enforcement partners understand the critical role they play in identifying and reporting suspicious activity to FSLTT law enforcement. These partners include:

- **Fire and Emergency Medical Services (EMS) Professionals** - Fire and EMS personnel have a significant reach into communities across the United States. In their efforts to prevent and respond to life and property losses, firefighters and EMS personnel enter homes, businesses, vehicles, and other assets thousands of times each day and, as a result, may be exposed to behaviors and indicators of potential criminal and terrorist activities.
- **Public Safety Telecommunications Professionals** - Because 911 is the number most people in the United States call to obtain help in a police, fire, or medical emergency, 911 dispatchers and operators can play an important role in SAR awareness. They are in the unique position of receiving calls for emergency services and may be able to filter and prioritize information, identify luring tactics, and provide intelligence and warning to ensure public safety.
- **Emergency Managers** - The responsibilities of the emergency management community include working closely with operators and owners of critical infrastructure and key resources, responding to emergency situations, and gathering information about disasters.

^cFor more information, see the **SAR Process Implementation Checklist** at

https://www.dhs.gov/sites/default/files/publications/17_0315_NSI_SAR-Process-Implementation-Checklist.pdf



This places them in a unique position to observe suspicious activity—related behaviors and indicators that may be indicative of preoperational planning for terrorism-related acts.

- **Corrections, Probation, and Parole Officers** - Community corrections professionals are in a position to recognize criminal or potential terrorism activities—especially while these activities are in the planning phase—due to their interaction with offenders during post-release aftercare and supervision programs as well as their contact with offenders' families and friends.
- **Private Sector Security and Critical Infrastructure Personnel** - There are more than 2 million security officers who protect the nation's critical infrastructure, and these security stakeholders can be force multipliers for sworn law enforcement officers to help protect communities and recognize and report suspicious activities.
- **Public Health and Health Care Professionals** - The integration of public health and health care professionals into the SAR process can enhance the preparedness of these organizations across the country while supporting the prevention, protection, response, and recovery efforts of all homeland security partners. These professionals may encounter individuals who display suspicious activities during regular interactions with the public.

CONSIDERATIONS

- Establish a basic understanding of indicators that are common in those who are mobilizing to violence, partnering with community members to identify them.
- Educate public safety officers on SAR and implement a formal process to document SAR.
- Provide information on the process to all relevant stakeholders.
- Consider working with local fusion centers and FBI Joint Terrorism Task Forces (JTTFs) to facilitate a collaborative approach to the SAR process.
- Be aware that sometimes traditional criminal activities can be a useful means by which violent extremists fund their efforts and that they may be observable and reportable if paired with other indicators of violence extremism.
- Work with threat assessment and management teams to determine whether follow-up threat assessments should be conducted.
- Information gathering—reasonably indicative of preoperational planning associated with terrorism—to assess a target's physical attributes, security features, vulnerabilities, or personnel movements is a component of nearly all premeditated attacks and may be observable.
- Work to understand different agencies' roles and responsibilities and how to best work together.
- Provide and solicit feedback when reports result in action.

Report Suspicious Activity

To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports will be forwarded to the appropriate fusion center and FBI JTTF for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi.



RESOURCES

DHS

- The **DHS Violence-Prevention Resource Guide** provides an overview of DHS resources supporting targeted violence-prevention for partners in the field as well as grant and funding opportunities. https://www.dhs.gov/sites/default/files/publications/21_0903_dhs-violence-prevention-resource-guide.pdf
- **If You See Something, Say Something**® is a program designed to help raise public awareness of the indicators of terrorism and terrorism-related crime that emphasizes the importance of reporting suspicious activity to proper state and local law enforcement officials. <https://www.dhs.gov/see-something-say-something>
- The **National Threat Evaluation and Reporting (NTER) Office** advances homeland security partner abilities to identify, investigate, assess, report, and share tips and leads linked to emerging homeland security threats. It also provides technical assistance, resources, and training associated with best practices in developing and implementing threat analysis-related activities associated with NSI. <https://www.dhs.gov/national-threat-evaluation-and-reporting-office>
 - **Nationwide Suspicious Activity Reporting Initiative (NSI)** - <https://www.dhs.gov/nationwide-sar-initiative-nsi>
 - **Building Community Partnerships (BCP)** is a fact sheet that provides an overview of the BCP initiative, which was established to assist fusion centers and law enforcement agencies in engaging and developing productive relationships with the critical sector and community stakeholders they serve to enable partnerships to protect critical infrastructure and prevent of crime and terrorism. https://www.dhs.gov/sites/default/files/publications/16_1218_NSI_Building-Community-Partnerships.pdf
 - **NSI Hometown Security Partners** is an overview of the SAR Hometown Security Partners Training strategy, which provides SAR awareness training for partners with similar missions to those of law enforcement constituencies, or "hometown security partners." https://www.dhs.gov/sites/default/files/publications/17_0315_NSI_Hometown-Security-Partners.pdf
 - The **Online SAR Training for Law Enforcement and Hometown Security Partners** is a multifaceted approach designed to increase the effectiveness of SLTT law enforcement and public safety professionals—and other frontline partners—in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. The website contains training videos that are tailored toward partners who may observe suspicious activity in the course of their normal duties. <https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training>



- The **SAR Process Implementation Checklist** provides a simplified checklist for chief executives and senior leadership to implement a SAR process within their agencies. https://www.dhs.gov/sites/default/files/publications/17_0315_NSI_SAR-Process-Implementation-Checklist.pdf
- The **SAR Indicators and Behaviors** is a tool for analysts and investigators that details potential criminal or noncriminal activities that require additional information during the vetting process or investigation, as well as defined criminal activity and potential terrorism-nexus activity. When the activity involves behavior that may be lawful or is a constitutionally protected activity, the investigating law enforcement agency will carefully assess the information and gather as much information as possible before taking any action, including documenting and validating the information as terrorism-related and sharing it with other law enforcement agencies. https://www.dhs.gov/sites/default/files/publications/16_0208_NSI_SAR-Indicators-Behaviors-Tools-Analysts-Investigators.pdf
- The **SAR Indicators and Examples** is a resource that provides the 16 ISE-SAR indicators, their respective definitions, and examples of suspicious activity scenarios that correlate with each of the indicators. https://www.dhs.gov/sites/default/files/publications/15_0223_NSI_ISE-Functional_Standard_SAR.pdf
- **10 Ways To Integrate SAR Into Your Agency's Operations** provides a brief overview of ten strategies that can be implemented by any agency to allow for the timely sharing of SAR information and to integrate the SAR process into its own operations. https://www.dhs.gov/sites/default/files/publications/17_0315_NSI_10-Ways-Integrate-SSAR-Into-Agency-Operations.pdf
- The **Behavioral Threat Assessment Integration** assists FSLTT homeland security partners with integrating a [Behavioral Approach to Violence Prevention](#) into their processes for identifying and mitigating homeland security threats of targeted violence, regardless of motive. The cornerstone of this line of effort is the **Master Trainer Program**: a train-the-trainer initiative that certifies partners in the instruction of Behavioral Threat Assessment and Management techniques and best practices. <https://www.dhs.gov/btai>
- **State and Local Fusion Centers** are focal points for the receipt, analysis, gathering, and sharing of threat-related information. <https://www.dhs.gov/fusion-centers>

FBI

- **eGuardian** - The information captured in eGuardian is migrated to the FBI's internal Guardian system, where it is assigned to the appropriate squad or JTTF for further investigative action, as required. <https://fbi.gov/resources/law-enforcement/eguardian>



- **Behavioral Threat Assessment Center (BTAC)** is a national-level, multiagency, multidisciplinary task force focused on the prevention of terrorism and targeted violence through the application of behavior-based operational support, training, and research. Encouraging bystander reporting is one of their top missions. Requests for BTAC assistance can be made through the Behavioral Analysis Unit Coordinator in your local FBI Field Office. <https://www.fbi.gov/services/cirg>
- **Joint Terrorism Task Forces (JTTF)** comprised of US law enforcement and intelligence agencies who work together and use participating agencies' resources to preempt, deter, and investigate terrorism and related illicit activities. <http://www.fbi.gov/contact-us/field>
- **JusticeConnect** is a criminal justice network that facilitates information sharing, partnership development, and project management for federal, state, local, and tribal partners in a secure environment. FBI posts unclassified products—to include Situational Information Reports. JusticeConnect is accessible via the Law Enforcement Enterprise Portal (LEEP).
- **LEEP** is a secure, Internet-based information-sharing system for agencies involved in law enforcement, first response, criminal justice, CT, and intelligence. <https://www.cjis.gov/CJISEAI/EAIController>
- **Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks.** This report is a practical guide on assessing and managing the threat of targeted violence and contains concrete strategies to help communities prevent these types of incidents. <https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view>
- **Terrorism Online Tips** provides options for the public to submit an anonymous tip to the FBI or other federal agencies, to include: DHS, the Federal Trade Commission, the Drug Enforcement Administration, the Internet Crime Complaint Center (IC3), the National Center for Mission & Exploited Children, and the Treasury Inspector General for Tax Administration. <https://tips.fbi.gov/>
 - IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. <https://www.ic3.gov/>

NCTC

- **The US Violent Extremist Mobilization Indicators Booklet (2021 Edition)** is an NCTC, DHS, and FBI tri-seal product that provides a list of observable behaviors that could help determine whether individuals are preparing to engage in violent extremist activities. For inquiries or more information, contact mib@nctc.gov or visit <https://www.dni.gov/index.php/nctc-newsroom/nctc-resources/item/2272-u-s-violent-extremist-mobilization-indicators-2021>.





PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: LE FIRE EMS HEALTH ANALYSIS PRIVATE SECTOR DATE:

PRODUCT TITLE:



ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

