CrimeStoppers (CSUSA)Briefing
September, 2017

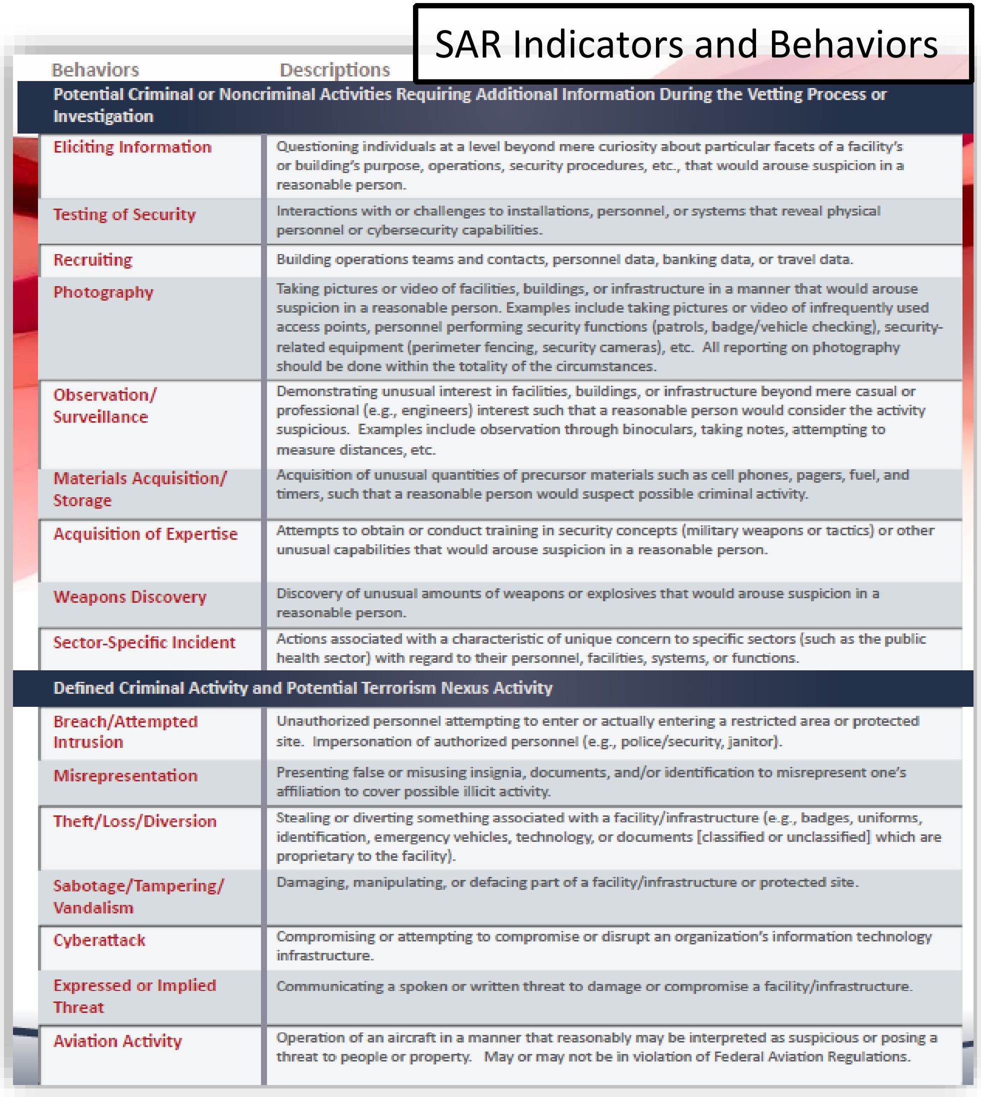
Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

NSI: The Need and Response

- Lack of terrorism-related information sharing among federal, state, local, tribal, and territorial law enforcement agencies
- Partnered with SLTT LE to define the needs, scope, and processes for suspicious activity reporting
- Used the SLATT® database, LAPD, and other local LE agencies to determine behaviors
- Developed the 16 **behaviors** that are potentially indicative of terrorism activity
- Decentralized, distributed system—allows local control and ownership of information (called for by federal law)
- Standards-based allows for information to be shared easily and seamlessly
- Built in privacy framework
- Partnership with the FBI’s JTTFs and fusion centers

NSI Process

- <u>Vetting and Submission</u>
  - Information submitted by law enforcement is reviewed by a trained analyst against the NSI Vetting Guidelines
  - Totality of the circumstances and interpretation of the behaviors
  - Functional Standard-compliant information is submitted to the NSI Federated Search and shared with other NSI users
  - Only the information determined by the local agency as shareable is available for search/view



SAR Indicators and Behaviors

Behaviors	Descriptions
Potential Criminal or Noncriminal Activities Requiring Additional Information During the Vetting Process or 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.

Purpose of START's NSI Research Project

- 1) What is the prevalence of terrorists' pre-incident activities aligning with existing SAR categories (or "SAR indicators"), and how does this vary by terrorism movement and crime type?
- 2) To what extent are SAR indicators observable versus actually observed,2 and how does this vary by terrorism movement and crime type?
- 3) How do SAR indicators relate to "successful" completion of terrorism cases?
- 4) What are examples of pre-incident activity committed by terrorists that do not fit within the 16 SAR categories and how prevalent are these activities?

START Research Findings

- 303 studied terrorist cases had an average of 7 instances of pre-operational behavioral indicators
- 80% (2,032 of 2,541) of the above pre-operational indicators aligned with the current 16 NSI behaviors
- In another study of 48 terrorist cases, only 49% (121 of 255) of the identified pre-operational indicators were deemed as “observable”
- Of the 121 observable indicators, 59% (72 of 121) were actually observed and reported.
- Terrorists involved in “acquisition” and “expressed threat” behaviors are far less likely to succeed

START Research Finding (cont’d)

- 20% (509 of 2,541) of the identified pre-operational indicators that were drawn from 303 terrorist cases did not align with the 16 NSI indicators
- Of the above 509 non-ISE SAR pre-operational indicators, the overwhelming majority involved one of the three following categories:

1) Meetings

2) Personal Communications (email & phone)

3) Travel

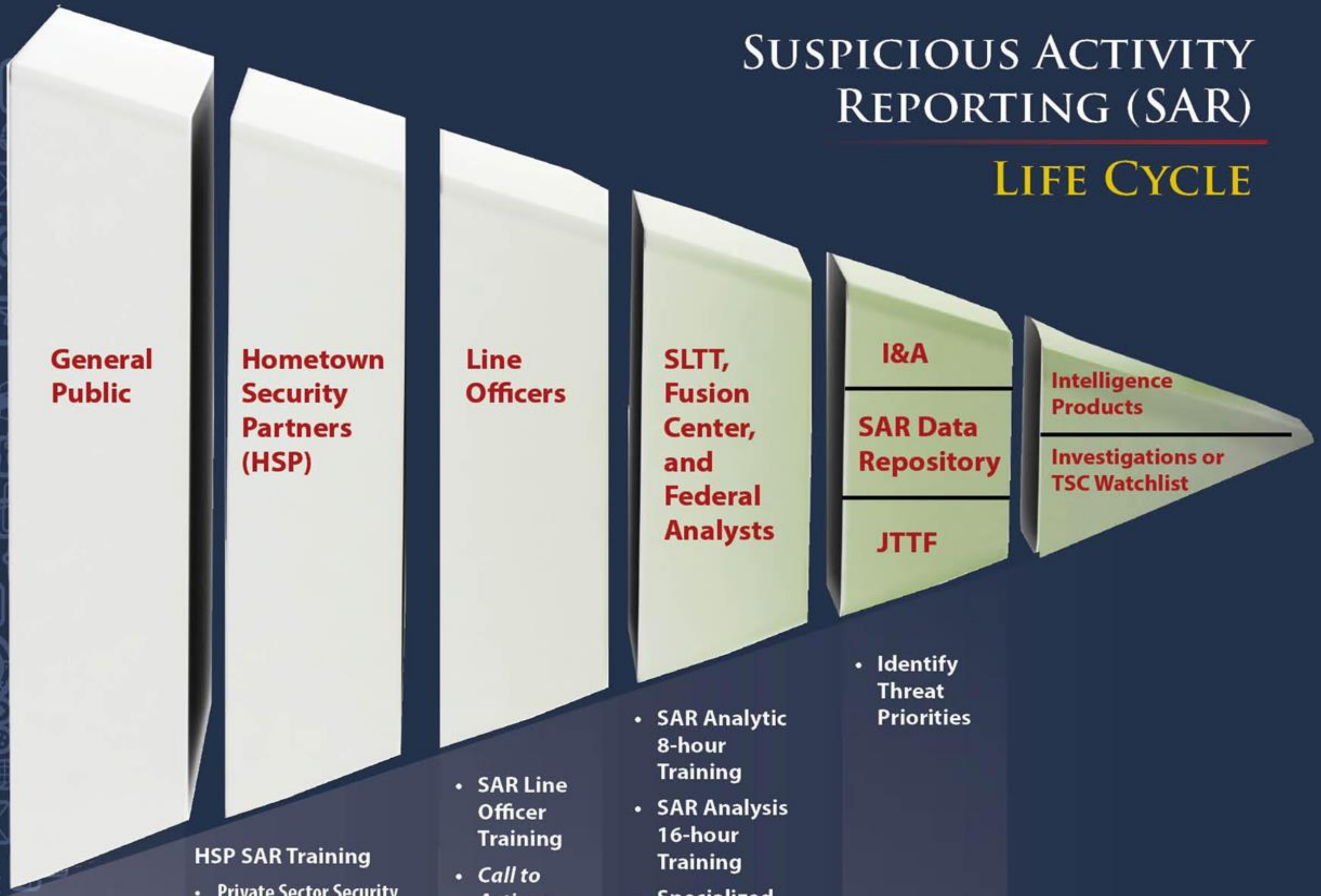
Lessons Learned From the START Report

- The NSI Process and its current 16 behaviors have been validated as an effective means to detect pre-operational activities linked to terrorism
- Less than half of the pre-operational indicators are observable and we are missing over 40% of those that are observable (identified gap)
- There are 7 specific pre-operational indicators that account for 79% (2,011 of 2,541) of all identified pre-operational indicators linked to 303 terrorism cases

Suspicious Activity Reporting (SAR) Life Cycle

Nationwide SAR Initiative NSI

Millions of Tips and Leads → Thousands of SARs → Hundreds of Investigations


General Public
Hometown Security Partners (HSP)
Line Officers
SLTT, Fusion Center, and Federal Analysts
I&A
SAR Data Repository
JTTF
Intelligence Products
Investigations or TSC Watchlist

How the NSI supports these efforts

General Public

- Building Communities of Trust
- If You See Something Say Something™

HSP SAR Training

- Private Sector Security
- Fire and Emergency Medical Services
- Probation, Parole, and Corrections
- Public Safety Telecommunications
- Emergency Management
- Maritime Sector

Line Officers

- SAR Line Officer Training
- *Call to Action: Unified Message*
- State and Local Anti-Terrorism Training (SLATT®)

SLTT, Fusion Center, and Federal Analysts

- SAR Analytic 8-hour Training
- SAR Analysis 16-hour Training
- Specialized Analytic Seminar Series

I&A / SAR Data Repository / JTTF

- Identify Threat Priorities

if you SEE something SAY something™

UNCLASS

Questions