Suspicious Activity Reporting
Indicators and Examples

Updated indicators and newly added examples from the February 2015 release of the ISE-SAR Functional Standard

DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY

BEHAVIORS/DESCRIPTIONS	EXAMPLES
BREACH/ATTEMPTED INTRUSION Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).	• At 1:30 a.m., an individual breached a security perimeter of a hydroelectric dam complex. Security personnel were alerted by an electronic alarm and observed the subject on CCTV, taking photos of himself in front of a "No Trespassing" sign and of other parts of the complex. The subject departed prior to the arrival of security personnel. • A railroad company reported to police officers that video surveillance had captured images of three individuals illegally entering a train station to gain access to a restricted-access tunnel and taking photos of the tunnel.
MISREPRESENTATION Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.	• A state bureau of motor vehicles employee discovered a fraudulent driver's license in the possession of an individual applying to renew the license. A criminal investigator determined that the individual had also fraudulently acquired a passport in the same name and used it to make several extended trips to countries where terrorist training has been documented. • An individual used a stolen uniform from a private security company to gain access to the video monitoring control room of a shopping mall. Once inside the room, the subject was caught trying to identify the locations of surveillance cameras throughout the entire mall.
THEFT/LOSS/DIVERSION Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.	• A federal aerospace facility reported a vehicle burglary and the theft of an employee's identification credential, a secure ID token, and an encrypted thumb drive. • An explosives ordnance company reported a burglary of a storage trailer. Items stolen included electric initiators, radios, and other items that could be used in connection with explosives.
SABOTAGE/TAMPERING/VANDALISM Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.	• A light-rail authority reported the discovery of a track switch that had been wrapped in a length of chain in a possible attempt to derail a passenger train car. • A natural gas company reported the deliberate removal of gas meter plugs on the "customer side" in two separate locations approximately a quarter of a mile apart. One location was a government facility. The discovery was made as the government facility's sensor detected the threat of an explosion.

DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY (CONTINUED)

BEHAVIORS/DESCRIPTIONS	EXAMPLES
CYBERATTACK Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.	• A federal credit union reported it was taken down for two and a half hours through a cyberattack, and the attacker was self-identified as a member of a terrorist organization. • A state's chief information officer reported the attempted intrusion of the state's computer network by a group that has claimed responsibility for a series of hacks and distributed denial-of-service attacks on government and corporate targets.
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.	• A customer-experience feedback agency received a call from a watchlisted individual stating, "Wait till they see what we do to the ATF, IRS, NSA." • 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 the U.S. Armed Forces.
AVIATION ACTIVITY Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.	• Federal air traffic control personnel reported two separate laser beam cockpit illumination incidents involving different commercial airliners occurring at night and during the take-off phase of flight. The reports revealed that the laser beam in both incidents originated from the same general geographic area, near a major airport on the East Coast. These findings indicate the likelihood of purposeful acts by the same individual. • A chemical facility representative reported an unauthorized helicopter hovering within 50 feet of a chemical tank located in a posted restricted area. An FAA registry search of the tail number was negative, indicating use of an unregistered number, which suggests an attempt to conceal the identity of the plane's owner and/or its place of origin.

POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL INFORMATION DURING VETTING

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, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A tour bus company servicing one of the nation's national monuments reported that a male subject asked a driver many unusual and probing questions about fuel capacity, fueling locations, and fueling frequency such that the driver became very concerned about the intent of the questioning. The male subject was not a passenger. • A guest services employee at a shopping center was questioned by an individual about how much security was on the property. The employee contacted security personnel, who confronted the individual. When questioned by security personnel, the individual quickly changed his questions to renting a wheelchair and then left without being identified. Security personnel reported that the individual seemed very nervous and that his explanations were not credible.

POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL INFORMATION DURING VETTING (CONTINUED)

BEHAVIORS/DESCRIPTIONS	EXAMPLES
TESTING OR PROBING OF SECURITY Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• An individual who refused to identify himself to facility personnel at a shipping port reported that he was representing the governor's office and wanted to access the secure area of a steel manufacturer's space. He was inquiring about the presence of foreign military personnel. The individual fled when he realized that personnel were contacting the security office about his activities. He ran through the lobby and departed in a vehicle with an out-of-state license plate and containing two other individuals. • An individual discharged a fire extinguisher in a stairwell of a hotel and set off the building's fire alarm. This individual was observed entering the hotel approximately two minutes before the alarm sounded, was observed exiting from the stairwell at about the same time as the alarm, and then was observed in the lobby area before leaving the hotel.
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.	• A prison inmate reported an effort to radicalize inmates nearing release toward violence. According to the plan, released inmates would go to a particular location for the purpose of obtaining information about attending an overseas terrorist training camp. • 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.
PHOTOGRAPHY Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.	• A citizen reported to local police that she saw an unknown male crouched down in the back of an SUV with the hatchback open half-way. The subject was videotaping a National Guard readiness center. The vehicle was parked on the side of the road but sped away when the citizen began to approach the vehicle. The citizen could not provide a license tag number. • A citizen observed a female subject taking photographs of a collection of chemical storage containers in the vicinity of the port. The subject was hiding in some bushes while taking photographs of the storage tanks. The citizen reported this information to the city's port police. When the port police officer arrived and approached the subject, she ran to a nearby vehicle and sped off.
OBSERVATION/SURVEILLANCE Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.	• 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. The subject became nervous when he detected security personnel observing his behavior. Once detained, the subject explained that he came to the mall to walk around and was simply videotaping the mall for his brother. The camera contained 15 minutes of mall coverage and footage of a public train system, along with zoomed photos of a bus. • Military pilots reported that occupants of multiple vehicles were observing and photographing in the area of residences of the military pilots. The pilots are responsible for the transport of special forces units. The report was made once the pilots realized that they had been individually surveyed by occupants of multiple vehicles during the same time period.

POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL INFORMATION DURING VETTING (CONTINUED)

Behaviors/Descriptions	Examples
Materials Acquisition/ Storage Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A garden center owner reported an individual in his twenties seeking to purchase 40 pounds of urea and 30 pounds of ammonium sulfate. The owner does not carry these items and became suspicious when the individual said he was purchasing the items for his mother and then abruptly departed the business. • A female reported that a man wanted to borrow her car to purchase fertilizer to add to the 3,000 pounds he had already acquired. When asked why he was acquiring fertilizer, he responded that he was going to "make something go boom." The subject lives in a storage unit and utilizes several other storage units at the location.
Acquisition of Expertise Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A fusion center received information on a watch-listed individual who was making repeated attempts to gain a hazardous materials endorsement for his commercial driver's license even though his immigration status made him ineligible. • A complaint was received from a gun shop about an individual under the age of 21 who had brought multiple groups of students into the gun shop to rent weapons to shoot. They desired to shoot assault rifles and handguns and asked questions about how to get around state and federal laws on weapon possession and transport.
Weapons Collection/ Discovery Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A city employee discovered a backpack near a park bench along the route of a planned Martin Luther King Day march in the city. The backpack contained an improvised explosive device. • A suspicious person call resulted in the discovery of three individuals possessing hand-held radios, a military-grade periscope, a 7mm Magnum scoped rifle, an AK-74 assault rifle, a pistol-gripped shotgun, a semi-automatic handgun, a bandolier of shotgun ammunition, dozens of loaded handgun magazines, dozens of AK-74 magazines, Ghillie suits, several homemade explosive devices constructed of pill bottles, blast simulators, and military clothing.
Sector-Specific Incident Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.	• A water company reported that it had security footage of an unknown person breaking into the premises. At 5 a.m., the individual cut through a fence and used a tool to breach a door. Once inside the building, the person took photos of the chlorination system, including the chlorine tank. A pump failure occurred, but it was not certain that this was related to the break-in. • A vehicle containing two individuals was discovered in a secure area of a loading dock at a facility that stores officially designated sensitive chemicals. The vehicle sped off upon discovery by security personnel. Surveillance footage revealed that the individuals gained entry by manually lifting a security gate to the compound.

The complete Functional Standard is available at http://ise.gov/sites/default/files/SAR_FS_1.5.5_IssuedFeb2015.pdf.

This project was supported by Grant No. 2011-MU-BX-K006 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.