SUSPICIOUS ACTIVITY

Preventing another terrorist attack in the United States continues to be one of the main missions of DHS. Ensuring that malicious actors cannot conduct terrorist attacks within the United States, and managing risks to our critical infrastructure and key resources, helps us realize our vision of a more secure and resilient Nation. In order to support this counterterrorism mission, each individual, business enterprise, and government agency must remain vigilant and report suspicious activity to law enforcement.

Suspicious Activity Reporting (SAR) is one of our best defenses against terrorist threats and our greatest resource to building resilience. Every day, members of the public work with law enforcement officers to help keep our communities safe by reporting activities that are out of the ordinary and suspicious. It is critical that law enforcement officers at all levels of government – state, local, tribal, territorial, and federal – who observe suspicious behaviors or receive reports from concerned civilians, private security, and other government agencies share this information with state and major urban area fusion centers, the Federal Bureau of Investigation, and other law enforcement agencies to help prevent future terrorist activity from occurring.

An aware and engaged public that understands what constitutes unusual and suspicious behavior is essential to protecting our communities from terrorist threats. For example, maybe you are at a high profile location or, perhaps a sporting event and you notice a person nearby taking several photos. While that is not unusual, you may also notice that the person is only taking photos of the locations of surveillance cameras, entrance crash barriers, and access control procedures.[1] That type of activity would be unusual. The following are examples of other unusual activities that should cause a heightened sense of suspicion:

- 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. 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. Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
- Abandoned packages constitute an implied threat due to the unknown nature of the contents.

Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).

[1] Information excerpted from the National Terror Alert Response Center. http://www.nationalterroralert.com/suspicious-activity/

- Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
- 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).
- Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
- Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
- Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
- Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
- 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
- Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.

Protective Measures

Many different protective measures are available for deployment at a facility and in the areas surrounding a facility. Some are applicable to a wide range of facilities and against a number of threat streams, while others are designed to meet the unique needs of a specific facility or a specific threat stream. In addition, some may be tactical in nature, while others may address long-term strategic needs. Examples include:

General Security

- Restrict access to authorized personnel only; assign ID badges with photographs; ensure accountability for lock and key control

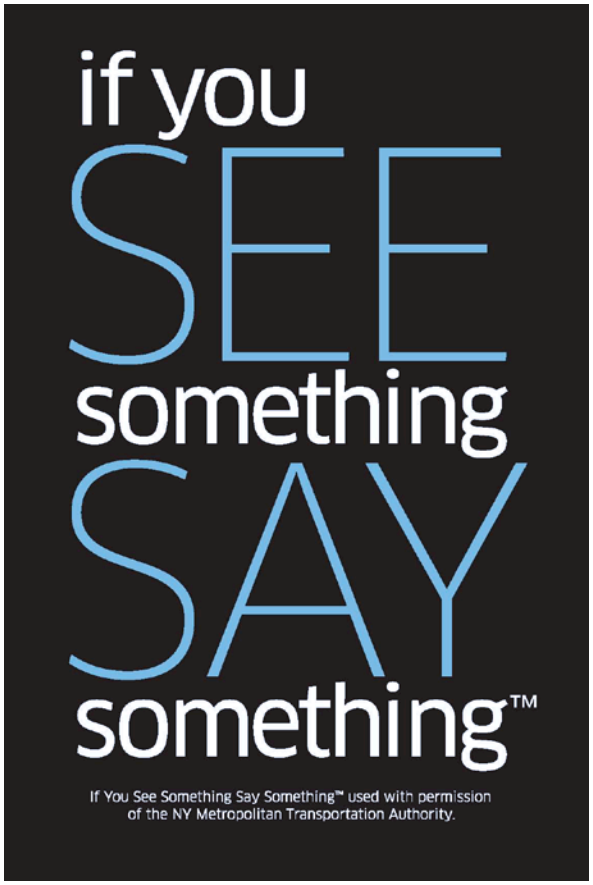
- Provide appropriate signs to restrict access to nonpublic areas.
- Have security personnel greet all employees and visitors and examine their personal belongings
- Install a security/fire alarm system and associated security service; install CCTV to record operation area and exterior entrances
- Ensure adequate lighting for the operations area, building exterior, and CCTV

- Screen all incoming mail offsite if possible; contact local law enforcement if a package is determined to be suspicious
- Ensure accountability for lock and key control.
- Develop an emergency plan for response to a known or a suspected hazard
- Restrict drivers and deliveries to a specific area.
- Establish a communication channel to report security deficiencies

Planning and Preparedness

- Designate an employee as a security director to develop, implement, and coordinate all security-related activities
- Develop a comprehensive security and emergency response plan
- Establish liaison and regular communication with local law enforcement
- Establish procedures to implement additional protective measures as the threat level increases

The DHS *"If You See Something, Say Something™"* Campaign



In July 2010, the Department of Homeland Security (DHS), at Secretary Janet Napolitano's direction, launched a national "*If You See Something, Say Something*™" public awareness campaign –a simple and effective program to raise public awareness of indicators of potential terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-crime efforts. To date, DHS has launched the "*If You See Something, Say Something*™" campaign in coordination with: Amtrak; the General Aviation community; the Washington, D.C. Metropolitan Police Department; the Washington Metropolitan Area Transit Authority (WMATA); the U.S. Tennis Association; the New York Mets; Meadowlands Stadium; the American Hotel and Lodging Association; New Jersey Transit; the Mall of America; Walmart; the National Football League (NFL); the National Basketball Association (NBA); NCAA and a variety of states.

For a full list of partnerships and for additional information about the campaign please go to www.dhs.gov/IfYouSeeSomethingSaySomething

The Office of Infrastructure Protection (IP) leads the national effort to mitigate risk to America's critical infrastructure from the full spectrum of 21st century threats and hazards. IP coordinates with government and critical infrastructure owners and operators across 18 diverse sectors to enhance critical infrastructure resilience, strengthen protective programs, and share vital information.