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

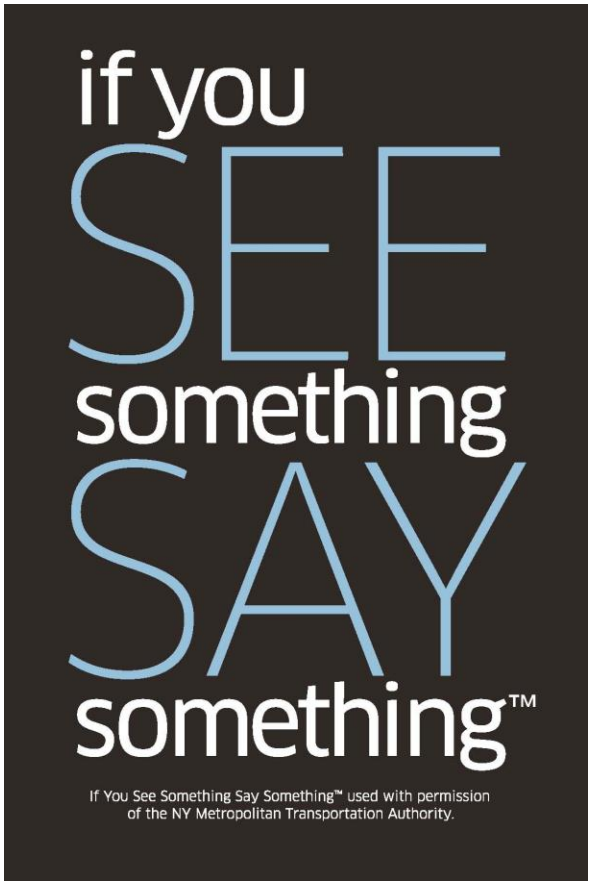
- Provide appropriate signs to restrict access to nonpublic areas.
- Have security personnel greet all employees and visitors and examine their personal belongings
- Install a security/fire alarm system and associated security service; install CCTV to record operation area and exterior entrances
- Ensure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

Office of Infrastructure Protection

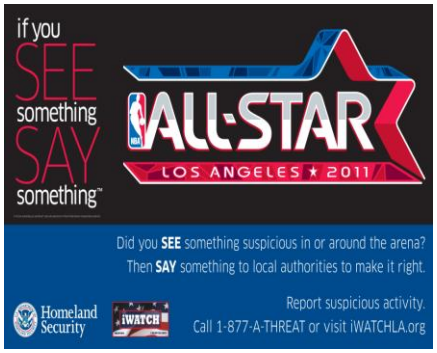
"If You See Something, Say Something™" Information and Public Display Materials

Homeland Security

In order for the Department of Homeland Security (DHS) to assist State, local, tribal, territorial and private sector partners with obtaining "*If You See Something, Say Something*™" materials the Office of Public Affairs will need to obtain specific information in order to draft materials – that information is outlined below. The Office of Public Affairs will send the draft(s) back to the requestor for final approval.

A few things that DHS will need to develop posters and other materials (might not apply to all materials):

- *What number should be called to report suspicious activity?*
- *What logos or images will appear on the materials?*
  - The DHS Logo must be on the image.
  - DHS prefers no more than three logos be used; however four can be included if necessary.
- *Format for logos*
  - DHS requires the logos in Encapsulated PostScript (EPS) format.
  - This format is a very high resolution and when printed produces the clearest image.



- *Size(s) of the final product*
  - DHS can mock up any size that you would like, please identify the size(s) (ie 11 X 17; 24 X 36, etc.)
- *Images on the poster*
  - Products traditionally use images that are local to the area or specific to the event.
  - If you would like more than one mock up, with different images, DHS can do that as well.
- *Format of final product*
  - Depending on how you will print the products, the format may vary.
- *Getting Final Products to you*
  - DHS can mock up and provide electronic copies so you can do in house printing and retain them for future use.
- *Location of final products*
  - Please identify the locations that the final products will be posted in. (Will they be in public spaces or areas for employees only?)

- *Product Options*
  - Posters, paystub inserts, table tent cards – if you think of something else just let us know what it is and size that is needed (ie: 11 X 14, etc.)
  - Electronic materials such as Ribbon Board/ Score Boards (just need pixels/dimensions to design)
  - Placing "*If You See Something, Say Something* ™" logo on credentials
  - Public Service Announcement – DHS can write the script for the Public Service Announcements. It is recommended that someone recognizable from your group record the message.
  - "Back-of-house" materials – These will help instruct staff/volunteers on what to look for and what they should do in case they see something suspicious.
- *Cost*
  - DHS does not charge partners to join the campaign, we can assist (at no cost) to develop products and provide electronic copies of materials for you to print.

www.dhs.gov/IfYouSeeSomethingSaySomething

For more information please contact:

- Sara Kuban, Director, External Engagement, Office of Public Affairs
  - Sara.kuban@dhs.gov; (202) 282-9840

FACT SHEET
Office of Infrastructure Protection

Homeland Security

Nationwide Suspicious Activity Reporting Initiative (NSI)
"If You See Something, Say Something™"
State and Major Urban Area Fusion Centers

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)

The findings in the 9/11 Commission Report and the Markle Foundation report clearly demonstrated the need for a nationwide capacity to share information that could detect, prevent, or deter a terrorist attack. The Intelligence Reform and Terrorism Prevention Act (IRPTA) of 2004 and the 2007 National Strategy for Information Sharing indicate both legislative and executive intent to establish locally controlled, distributed information systems wherein potential terrorism-related information could be contributed by the 18,000 state, local, tribal, and territorial (SLTT) law enforcement agencies for analysis to determine whether there are emerging patterns or trends. Following this guidance, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) was created. The NSI has established standards, policies, and processes for gathering, documenting, processing, analyzing, and sharing SAR while taking into account the protection of privacy, civil rights, and civil liberties of Americans. Behaviors that may not seem suspicious in and of themselves, when combined with other actions and activity, could be indicative of terrorist activity. The ability to share this information about suspicious activity is critical to law enforcement, from the officer on the street to supporting analysts. Through the efforts of the NSI – led by the U.S. Department of Justice and working in coordination with the Federal Bureau of Investigation and the Department of Homeland Security – the ad hoc methods of reporting and analysis cited in the 9/11 Commission Report have been standardized and policies and processes put in place so that timely, relevant information can be shared between state, local, tribal, and federal law enforcement agencies. For more information on the NSI please visit: http://nsi.ncirc.gov/.

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.

State and Major Urban Area Fusion Centers and Suspicious Activity Reporting

DHS works closely with the Department of Justice-led Nationwide Suspicious Activity Reporting Initiative Program Management Office to establish a standard process to identify and report suspicious activity in jurisdictions across the country. With the Office of Intelligence and Analysis (I&A) leading the way, DHS has made it a priority to participate in and support the implementation of the NSI while also integrating SAR processes across the National Network of Fusion Centers. The integration of NSI within both DHS and the fusion centers is a key element of coordinated outreach to homeland security stakeholder communities across the country.

Protective Security Advisors (PSAs) and the Enhanced Critical Infrastructure Protection (ECIP) Program

PSAs from the DHS Office of Infrastructure Protection, Protective Security Coordination Division, conduct security assessments and surveys of nationally significant critical infrastructure, known as Level 1 and Level 2 facilities, through the Enhanced Critical Infrastructure Protection (ECIP) program. The goals of the

ECIP program are to assess overall security postures and recommend protective security measures at Level 1 and Level 2 facilities; to inform facility owners and operators of the importance of their facilities and threats from terrorism; and to develop strong relationships between critical infrastructure owners and operators, DHS, and Federal, State, Local, Tribal and Territorial law enforcement and intelligence communities. PSAs reside and work in communities across the country. They play a vital role in supporting National level homeland security initiatives such as the Nationwide Suspicious Activity Reporting, the DHS "*If You See Something, Say Something™*" Campaign, and the National Network of Fusion Centers by conducting outreach activities to educate and inform members of their stakeholder communities.