Terrorism Threat Awareness Training for Security Officers

Vigilance

means being watchful and alert, especially when attempting to guard against security threats and safety risks. Along with *integrity* and *helpfulness*, it is one of the three core values of Securitas. Vigilant security officers can frequently help to identify threats and hazards before they become problems. Security officers frequently discover problems before they get bigger. Through training and experience, security officers can also gain insight into what is usual and what is not at their jobsite. This is an especially valuable skill in guarding against terrorism threats.

Terrorism Defined

Terrorism can be defined in a number of ways. In the most direct terms, terrorism is a deliberate, criminal use of violence against people or property for political, social or religious ends. Acts of terrorism can come from domestic sources sometimes referred to as "homegrown" terrorism. Homegrown terrorism is when a person or group in the United States receives support solely from individuals and organizations, also in the United States, and commits attacks within the United States.

International terrorism involves attacks within the United States that are committed by individuals or groups that originate outside the United States or that are influenced or supported by foreign interests. Most terrorist incidents in the United States are perpetrated by domestic terrorists.

Terrorist Aims and Targets

Terrorists use violence and threats of violence to instill fear in the population for the purpose of forcing change. They aim to advance their position by killing as many people as possible and by achieving strong emotional responses from the population affected by their attacks. To achieve these goals, terrorist acts may be more likely to occur at locations where large numbers of people gather or at a time or place where an attack would have a far-reaching or newsworthy impact.

Ideal targets for terrorists include sites with major historical, cultural, religious, or other symbolic importance. These include government facilities, iconic landmarks, events, or places where large numbers of people gather, sensitive facilities or resources—like nuclear plants or food and water supplies, and sites that represent core values and primal emotions—like daycare centers or elementary schools. However, the reality is that terrorist attacks have the potential to happen anytime and anywhere.

In addition, terrorist attacks are often planned for specific dates that carry emotional weight, like the anniversary of other terrorist attacks or the celebration of unique American events like Independence Day or the Super Bowl.

Guarding Against Terrorist Threats

The first step in guarding against and mitigating terrorist threats is to be prepared. This involves knowing about terrorism threat alert systems and how they may affect security procedures at your site; understanding procedures outlined in the client's facility security plan; and following your post orders.

National Terrorism Advisory System (NTAS)

In 2011, the Department of Homeland Security introduced the National Terrorism Advisory System, or NTAS, to replace the color-coded threat level scale that had been in place since 2002. Under NTAS, DHS will issue detailed alerts to the public when the federal government receives information about a credible terrorist threat.

Using available information, the alerts will provide a concise summary of the potential threat, including, if available, the geographic region, mode of transportation or critical infrastructure potentially affected by the threat; information about actions being taken by authorities to ensure public safety; and recommended steps that individuals, communities, businesses, and governments can take to help prevent, mitigate, or respond to the threat.

NTAS alerts will only be issued when credible information is available. They will inform the public and relevant government and private sector partners about potential or actual homeland security threats. NTAS alerts include a clear statement on the nature of threat, which will be defined as either "imminent" or "elevated."

An Elevated Threat Alert warns of a credible terrorist threat against the United States. An Imminent Threat Alert warns of a credible, specific, and impending terrorist threat against the United States.

Other Terrorism Alert Systems

In addition to NTAS alerts, some facilities may also be affected by industry-related threat level systems. For instance, the Maritime Security System (or MARSEC)—under the control of the U.S. Coast Guard—regulates sites located at ports or along waterways and facilities where products come in or go out by freighter, tanker or barge. The Chemical Facilities Anti-Terrorism Standards (or CFATS) regulates various sites where chemicals are manufactured, distributed, stored and used. In addition, some clients may employ their own site-specific threat level system.

Depending on the unique features of the security assignment, it is helpful if security officers are aware of the threat level alert systems in affect at the site and how security procedures and responsibilities change when an alert is issued or there is a change in threat level. Threat-response procedures vary from site to site. Site-specific security measures are directed by the Facility Security Plan, the post orders, instructions from the supervisor, or the Facility Security Officer.

Terrorist Precursor Conduct

Depending on the unique features of the security assignment, Security officers should attempt to be aware of suspicious people, vehicles, things, and items. Certain kinds of activities are more likely to indicate that terrorist plans are being planned, especially when they occur at or near high-profile sites, at places where large numbers of people gather, or anywhere while a threat alert is in place.

The Department of Homeland Security (or DHS) has identified specific "precursor conduct" to watch for. Precursor conduct is suspicious behavior and activity that may signal terrorist planning.

DHS Categories for Terrorist Precursor Conduct

The DHS categories for terrorist precursor conduct are: *Surveillance; Deploying Assets; Suspicious Persons; Suspicious Questioning; Tests of Security; Acquiring Supplies;* and *Dry Runs.* Let's take a closer look at each of these suspicious behaviors and activities.

Precursor Conduct: Surveillance

Surveillance generally involves observing a target area off and on over an extended period of time during the planning phase of an operation. Surveillance is conducted to determine the strengths and weaknesses of the target, to establish a strategy for the attack, and to assess the likelihood that the attack will succeed. It is helpful if security officers are alert for vehicles that repeatedly drive by the area—especially vehicles moving slowly and whose occupants seem to be unusually focused on the site. It is also helpful if security officers are alert for loiterers at or around the site, or anyone who makes repeated short visits to the site, but does not seem to have a legitimate business purpose. Security officers should also attempt to be aware of people recording or monitoring activities, taking notes, drawing maps, or using cameras, binoculars, or other observation equipment at or near the site. Being aware of suspicious surveillance activity is sometimes as simple as using common sense and being aware of unusual activities or things that do not appear to be normal objects at the site.

Precursor Conduct: Deploying Assets

Terrorist precursor conduct often includes deploying assets and getting resources into position to carry out the attack. This might involve abandoning vehicles or objects near or at the target site; stockpiling suspicious materials; or positioning people near a key facility.

Precursor Conduct: Suspicious Persons

As a security officer, you should always try to be alert for suspicious people and behaviors. What makes a person suspicious? In the simplest terms, anyone who does not seem to fit in at the site or through common sense arouses suspicion. This is especially true if you work at a post where you are likely to know everyone, like in a highly-restricted area or small-sized campus dormitory. In more general terms, a suspicious person is anyone who does not appear to belong in the workplace, neighborhood, and business establishment or near a key facility, or anyone whose behavior or appearance seems out of place.

A good way to detect suspicious people and their behaviors is to know the environment. It is helpful if a security officer gets to know the people at the site. When you are on patrol or at your site, try to remain alert and become familiar with the normal patterns of movement, typical attire, common activities, and the kinds of individuals who are regularly on site. By closely observing the people who come and go over time, you can become more skilled at spotting those who may not belong. Remember that determining whether a person is suspicious depends on that individual's behavior. **It is not based on the person's ethnicity, race, religion, or those kinds of factors.**

Precursor Conduct: Suspicious Questioning

Terrorist precursor conduct often involves information gathering. Try to be alert for anyone attempting to gain detailed information in person, by phone, mail, email, or other communication method regarding a site or its personnel—especially at a key facility. For example, an unauthorized person attempting to gain in-depth knowledge about a critical infrastructure like a power plant, water reservoir, or a maritime port would be cause for suspicion. Terrorists may try to gain information about site logistics, make unusual inquiries concerning shipments, or ask questions about security and other business operations. They may also attempt to place "key" people in sensitive work locations. It could be a warning sign if someone starts asking probing questions about the facility or about sensitive information that falls outside his or her area of responsibility.

Precursor Conduct: Tests of Security

Terrorist planning may also involve attempts to penetrate or test physical security or security procedures at the target site. A suspect may attempt to enter the site without proper access control authorization in order to see if it is possible to successfully do so; to determine how far he or she can get before being detected or turned away; or to observe first-hand the actual procedures that take place at various access control points across the site. Tests of security might also involve attempts to enter the site through alternate or secondary access points in order to find a weakness in site security. Try to be on the lookout for individuals who appear from unusual directions.

Tests of security can give terrorists information about existing weaknesses in security at a site. In addition, if an attempt is unsuccessful, terrorists may learn useful information about security response procedures—like how many security officers responded to the incident (and where they came from)—or how long it took for authorities to arrive and what route they took.

Precursor Conduct: Acquiring Supplies

Prior to a terrorist act, terrorists may attempt to buy or steal weapons, explosives, or ammunitions. They may attempt to gather the supplies to make them; such as large amounts of ammonium nitrate fertilizer, hydrogen peroxide, chlorine, or other potentially dangerous chemicals. Terrorists may also attempt to acquire official vehicles, law enforcement, or military uniforms and badges, or other materials that may help them pose as authorized personnel.

Try to be alert for anyone who attempts to steal forms of identification like access cards, drivers' licenses, passports, or the supplies to counterfeit them. Possessing proper forms of identification could greatly increase terrorists' chances of gaining entrance onto a site or into sensitive or restricted areas.

Precursor Conduct: Dry Runs

Another terrorist indicator to watch for is a "practice run" or a "dry run" aimed at your facility. Often, before the execution of the final operation, a terrorist cell will run one or more practice sessions to work out flaws and unanticipated problems in the attack plan. Behavior that may be preparation for terrorist activity includes mapping out routes, playing out scenarios with other people, monitoring key facilities, or determining the timing of traffic lights and traffic flow. Dry runs may very well be at the heart of the planning phase of a terrorist act. The Department of Homeland Security reports the best chance to intercept and stop a terrorist attack is during this stage.

It is helpful to know the signs of precursor conduct and to be watchful for them while on post and on patrol.

Reporting Precursor Conduct

The first step in guarding against a terrorism threat is knowledge; knowing what to look for. The second, and equally crucial step, is reporting.

If you see anyone that you think may be engaged in behaviors or activities that may indicate terrorist planning, report it immediately. Follow the procedures in your post orders for responding to and reporting precursor conduct. This may involve alerting the client contact, your supervisor, local law enforcement, the FBI or the nearest Joint Terrorism Task Force. If there is an emergency or an immediate threat, call 911.

The ability to recognize and report intelligence gathering activities and other precursor conduct may interrupt potential terrorist events, crimes, and other threats before they occur.

It is important to remember that terrorist planning can span an extended period of time, and weeks, or even months may pass between instances of precursor conduct. In addition, these planning actions may occur months—or quite possibly years—before the terrorist act itself. Therefore, it is extremely important to accurately document your observations. Your documentation of suspicious activities and behaviors could potentially provide information which authorities use to "connect the dots" and disrupt a possible terrorist attack.

This guide is for informational purposes only and does not contain Securitas USA's complete policy and procedures.

For more information, contact your Securitas USA supervisor or account manager.