CHEMICAL SECURITY MONITOR

A Free Publication of Critical Intervention Services, Inc. Fall 2002

The Chemical Security Monitor is a free publication of Critical Intervention Services. All articles featured in this publication are authored by CIS Special Projects personnel.

Critical Intervention Services
Special Projects Office
1261 South Missouri Ave.
Clearwater, Florida 33756
Tel. (727) 461-9417 • Fax (727)449-1269.
Email: chemical_security@cisworldservices.org

Critical Intervention Services is a Florida-based company providing a range of consulting,training,and protective services to businesses and governments throughout the world. Founded in 1992,CIS is an industry leader in developing and incorporating advanced solutions for security-related problems.

Contents

Beyond the CWC and FBI Community Outreach Lists:

Additional chemicals worthy of protection as possible CW agents and precursors

By the CIS Special Projects Staff

In the aftermath of the events of September 11th, companies in the United States have been encouraged to ensure adequate protection of chemicals with possible use as chemical warfare (CW) agents or agent precursors. The theft of chemical agents or precursors by malevolent adversaries has been identified as one of the four key security events by the Center for Chemical Process Safety (CCPS) in the new CCPS Security Vulnerability Assessment program. The American Chemistry Council (ACC) has also identified this risk as one of the issues of concern in the revised security code for the Responsible Care program. To aid companies in identifying potential CW agents and precursors, both organizations refer to two primary sources.

The first source, the CWC/Australia Group list, identifies specific chemicals and families of chemicals that have application as previously weaponized CW agents or in the production of classic CW agents such as sarin, VX, mustard, and lewisite. The CWC list also includes several biological toxins with known potential for weaponization. The Australia Group list, which is largely based on the CWC list, also contains an expanded list of living and non-living agents of biological origin. For the purpose of prioritization, the Chemical Weapon Convention (CWC) organizes toxic chemicals and precursors into three "schedules" and an additional category of "unscheduled discrete organic chemicals" (UDOCs).

The second source referred to by CCPS and ACC is the FBI Community Outreach list. This list includes 42 chemicals with properties that the FBI has determined to pose significant risk of terrorist or criminal misuse. The FBI's list includes a number of chemicals identified on the CWC list, plus a number of common toxic industrial chemicals and chemicals that could aid in the delivery of toxic agents (such as DMSO).

In general, the CWC/Australia Group list and the FBI Community Outreach list provide an excellent starting point for identifying chemicals that may require heightened theft controls. However, both lists fall short in identifying the full spectrum of chemicals that could be attractive as terrorist agents or precursors. To appreciate this fact, it is first necessary to understand the criteria that was used for developing the lists.

The CWC/Australia Group list only includes chemicals that were identified as CW agents or agent precursors prior to the signing of the CWC in 1993. All of the agents addressed by the CWC were previously weaponized or standardized as military chemical warfare agents. The CWC list fails to address a number of experimental chemical agents and CW agents that were secret at the time of the convention. One example of this is the novichok family of Russian third-generation nerve agents. In 1993, the existence of the highly toxic novichok agents and their precursors was classified. Today it is public knowledge that at least one novichok variant (A-234) is a simple unitary agent derived from aconitrile and a common organophosphate pesticide precursor. At the present, neither aconitrile or the pesticide precursor appear on the CWC or FBI list.

In addition to the novichok variants, there are a number of experimental chemical agents that were developed by governments that do not appear on the CWC or FBI lists. Though many of these agents are closely related to standardized CW agents, the precursors for many experimental agents (such as EA 1788 or EA2233) are unique and do not appear on the CWC or FBI list.

One of the reasons for the incomplete listing of possible agents and precursors is the common assumption that terrorists will focus their attention strictly on "lethal" or "militarily significant" agents. By contrast, there are a number of chemical agents that do not meet the typical criteria of "lethal" or "military" agents that may be quite attractive to terrorists due to their effects or ease of procurement. It is important to remember that the requisite characteristics of ideal military CW agents is very stringent. Issues such as production cost, stability in storage, and numerous other factors greatly limit the number of chemicals that a government may find attractive as CWagents. In general, terrorists are not bound by the same constraints. Likewise, the terrorist's primary goal may not necessarily be to kill or immediately incapacitate. Any chemical with appropriate dissemination characteristics and effects that may result in widespread public fear could be a possible terrorist agent.

A large number of agents exist with properties that terrorists may find attractive that most countries have largely rejected as military CW agents. One example is the fentanyl family of chemicals. Fentanyls are powerful opioid analgesics commonly used as narcotic medications or as designer street drugs. Examples of fentanyls include carfentanil, alfentanil, 3-methyl fentanyl, 3-methothiofentanyl, sufentanil citrate, and hydroxy methyl fentanyl. Fentanyls are exceptionally powerful pyschoactive chemicals with a relatively high level of toxicity. Their properties as incapacitants or potentially lethal agents has made fentanyls attractive as candidate CW agents to several countries including the US and the UK. Nevertheless, the precursors for fentanyls do not appear on the CWC list or the FBI list.

Another example of a chemical with potential terrorist applications is MPTP. MPTP is a contaminant that appears in poorly synthesized MPPP (a meperidine analog commonly used as synthetic heroin). MPTP intoxication produces a condition called "chemically-induced Parkinson's Disease." The symptoms appear as a rapid onset of Parkinson's Disease with often irreversible chronic effects. Though most cases of MPTP poisoning are unintentional, terrorists could easily prepare concentrated MPTP by exaggerating the conditions during synthesis that result in accidental MPPP contamination. The primary precursor required to produce MPTP, 1-methyl-4-peperidone, is not listed by the CWC or the FBI as a possible CW agent precursor.

Overall, it is estimated that there are approximately 300-500 chemicals with properties that may be attractive to terrorists (not including common industrial

chemicals released in large quantity). Some experts estimate that this number is conservative, and that there may be as many as 1,000s of possible terrorist CW agents and precursors. We hope that ACC and CCPS will eventually expand the list of chemicals requiring prioritized theft-protection to include more of these potential terrorist CW agents and precursors. In the meantime, companies are encouraged to re-examine their inventories to identify other possible chemicals at risk. As a minimum, companies should be aware of the possible malevolent motives behind chemical theft and establish a procedure for reporting suspicious losses of any chemicals (regardless of their list status) to the police and local FBI field office.

Australia Group List
http://www.australiagroup.net

FBI Community Outreach List
http://www.fbi.gov
http://www.costha.com/logs/pdf%20files/security&safety/ChemInfofbi.pdf

For assistance in identifying alternative CW agents/precursors, vulnerability assessment, or security planning,contact Critical Intervention Services: Tel. (727) 461-9417, or by email at chemical_security@cisworldservices.org

Bomb Threat Management for Chemical Facilities, Part 1

By Craig S. Gundry, CPS
Vice President of Special Projects, Critical Intervention Services

This article is reprinted in two-parts from the Chemical Plant Bomb Threat Planning Handbook, published by Critical Intervention Services. A free copy of the handbook is available by contacting CIS at chemical_security@cisworldservices.org.

Most traditional approaches to bomb threat planning rely on the assumptions that a facility has a relatively large security staff and operations that can be abandoned to permit a quick and complete evacuation. Unfortunately, these types of approaches do not account for the unique circumstances often present at chemical facilities. Issues such as process safety, security personnel deployment, facility size and layout, and dispersion of employees often limit the feasibility of adopting conventional bomb threat management strategies commonly used in offices and other environments.

This two-part article is written to aid security planners in developing effective bomb threat management protocols for chemical facilities. The methodologies described in this article are based on established principles and modified, as necessary, to account for the conditions present at most chemical manufacturing, storage, and distribution facilities.

Characteristics of Bomb Threats

Telephoned threats persist as the most common bomb-related problem faced by businesses and communities. Every year, thousands of threat calls are received by organizations ranging from large corporate offices to schools and churches. Fortunately, most of these threats are fictitious. In most locations, over 99% of bomb threats turn out to be either hoaxes aimed at instilling panic and disrupting a particular activity, or nothing more than thoughtless pranks—perpetrated for the caller's amusement.

Though it is tempting to dismiss all bomb threats as hoaxes, bombers do occasionally provide warning before attacks. In most of these cases, the bomber is trying to reduce the risk of casualties by providing a chance for evacuation. In this situation, the bomber often perceives killing or injuring innocent bystanders as counter-productive. Many

terrorists realize that a high number of civilian casualties often produces adverse publicity and may possibly alienate support for their cause. Moreover, many terrorists use bomb threats to ensure that proper credit is given to the group or to provide a rationale for the bombing. In many of these cases, the bomb threat is called in to a news organization, such as a newspaper or television station.

Though most authentic bomb threats are delivered with the intention of sparing innocent lives, some terrorist groups employ deceptive bomb threats as part of carefully planned operations designed to achieve specific strategic goals. In some of these situations, the bomb threat is used to deceptively lure people to the location of a bomb in order to create a high number of casualties. In other cases, the bomb threat may be crafted in such a way as to deliberately discredit police and emergency responders. Though malicious bomb threat situations are rare, it is important that security planners consider the possibility of these risks when developing facility response protocols.

Following is a description of a few of the most common "malicious" strategies associated with bomb threats.

1. The "Mousetrap"

A number of terrorist groups have used threat calls to deliberately target police and bomb disposal personnel. In this situation, the bomb threat is used specifically to lure bomb disposal technicians to the location of a boobytrapped or remote-controlled device. In the latter case, a terrorist observing from a nearby location activates the device once bomb technicians or police have entered the "kill zone."

2. False Bomb Location

The objective of this type of scenario is to cause maximum casualties (and public fear). In this situation, the bomber places the call with prior knowledge of how police or security will evacuate the area. A device is then concealed near the suspected assembly point or along the evacuation route. Once people have collected at the assembly point, the device explodes (activated by time delay or remote-control).

The 1998 bombing in Omagh, Northern Ireland was a dramatic example of this. In the Omagh incident, a caller told police that a bomb was located outside of the local courthouse. To verify his authenticity, the caller provided a code word known only to the IRA and British authorities. The police initiated an immediate evacuation of the surrounding area. Forty minutes later, as people began to assemble a safe distance away from the courthouse, 500 pounds of explosive detonated in the evacuation zone—killing 28 people and injuring 220 others.

3. Short Warnings

In this scenario, the terrorists deliver a warning with full awareness that the police will not have sufficient time to evacuate the area, identify the device, and safely dispose of it. This places the police in a difficult position. Despite their best efforts to respond, public attention after the attack easily shifts from the perpetrators to the police with speculations of "Why wasn't response more effective?". This increases public anxiety and erosion of the public's faith in the authorities. In addition to its psychological impact, short warnings increase risk to responders—particularly bomb technicians preparing or executing render safe procedures (RSP).

Planning Considerations

To manage the problem of bomb threats effectively, all chemical facilities should develop a bomb threat response plan.

Several issues need to be considered while a bomb threat response plan is being developed:

1. Level of Threat
2. Nature of the Organization's Structure and Activities
3. Critical Process Activities
4. Facility Layout

5. Outside Resources (law enforcement, canine search teams, etc.)
6. Access Vulnerability
7. Safety
8. Legal Issues

Level of Threat

Accurate threat assessment is essential in determining appropriate response actions to a bomb threat. For example, facilities with low levels of threat may decide to use searches of the work area by employees and to limit evacuations only to situations where a suspicious object is identified. Other facilities, with higher levels of risk, may decide on a full evacuation regardless of whether a suspicious object is identified or not.

Nature of the Facility's Structure and Activities

The facility's employee structure will determine who is responsible for different activities during a bomb threat. For example, a facility with a low number of security personnel may require considerable assistance from employees in searching various areas of the building. Additionally, the management structure will determine who will make the decision to evacuate or reoccupy the facility and how information will be communicated to employees.

Critical Process Activities

Critical process operations at the facility need to be considered in determining what activities can be shut down during a threat and what needs to remain in operation. If a critical activity cannot be stopped during a threat, what provisions can be made to ensure the safety of people and equipment required to sustain that activity during the initial response? Additionally, at what point does the activity need to be shut down and personnel evacuated? How long would it take to safely shut down a critical process operation? These are very important issues that need to be considered during the planning phase.

Facility Layout

The layout of the facility will dictate how search zones are assigned and where evacuation routes and assembly areas should be located.

Outside Resources

What resources from local law enforcement are available to assist with search and evacuation? In most locations in the United States, police respond only in the event that a suspect object is identified. In other locations, police may be willing to dispatch officers or a canine team to assist in searching the facility.

Access Vulnerability

How effective are existing security measures in preventing bombs from entering the facility? Organizations with open access to the public may need to search a location much more thoroughly than an organization with strong security measures. Conversely, facilities with well-developed access control and screening systems may wish to limit searches of secured areas while intensifying search of public locations outside the secured areas.

Safety

Safety is the most important consideration in conducting a bomb search. All procedures for search and evacuation should be carefully designed to minimize risk to the facility's occupants.

Legal Issues

A number of potential legal issues need to be considered when developing a bomb threat management plan. One of the most important of these issues is the role of non-security employees in bomb search and response activities. One approach to conducting a bomb search relies on employees to conduct complete searches of their work areas following a bomb threat. In unionized working environments, utilizing employees in this type of capacity may violate labor agreements. This is an issue that needs to be explored with legal counsel on a case-by-case basis.

Poor execution of the written search plan is another issue to consider. If an organization improperly executes a well developed and documented response plan, the organization may be exposed to law suits arising from negligence.

Bomb Threat Planning

There are several steps in developing an effective bomb threat plan:

1. Designate responsibilities.
2. Define procedures for handling threat calls.
3. Determine procedures for evaluating threat calls.
4. Identify an Incident Command Point (ICP).
5. Develop a search and evacuation plan.
6. Establish a response procedure.

Part One of this article continues with addressing steps 1-4 of the bomb threat planning process. Steps 5 and 6, search and response planning, will be fully explored in Part Two in the next issue of the Chemical Security Monitor.

Step One: Designate Responsibilities.

The first step in developing a bomb threat response plan is assigning an incident commander. This person will be responsible for evaluating the original threat, supervising search activities, ordering necessary evacuations, supervising response to any suspect objects, and determining when the facility can be reentered. In most cases, the senior security or safety manager is usually designated as the incident commander.

Additionally, alternative incident commanders should be designated in the event that the primary one is not present when a threat is received.

In addition to the incident commander, a communications network should be established through the organization's chain of command to ensure that employees are properly informed and supervised while responding to the threat. This chain of command usually works best if it mirrors the organization's existing management structure. To ensure that all parties are aware of their role, this communications network should be completely described in writing at the time the plan is developed.

In an ideal situation, an individual under the incident commander's supervision will notify all department supervisors or designated "floor wardens" of the bomb threat and instruct them to initiate the response procedure. Each activity supervisor or floor warden then notifies his employees of the threat and supervises their search or evacuation activities.

Step Two: Define a procedure for handling threat calls.

Most bomb threat calls are answered by a recipient on a telephone line with a publicly listed number. In smaller facilities, this usually limits the number of possible recipients to a handful of receptionists or switchboard operators. However, in many larger facilities, different offices may have publicly listed numbers answered by separate recipients. In either case, anyone responsible for answering a publicly listed telephone number should be trained in procedures for handling bomb threat calls. Moreover, each telephone used for receiving public inquiries should be furnished with a bomb threat card to assist employees in managing the call and recording information afterward. See the sidebar on page 7 for an example the types of information contained on a Bomb Threat Card.

When a threat arrives, the person receiving the call should remain calm and use the following procedure:

• The recipient should pay close attention to the caller's message. He/she should ask the caller to repeat the message and should be sure to record or note every word the caller says.

As a minimum, the recipient should ensure that the caller provides two vital facts:

1. Location of the Device
2. Time of Detonation

• If possible, the recipient should signal someone else in the room to listen in on the call. Many people are shocked when they receive a bomb threat and often overlook small details of the caller's statements. Two people will have a much better chance of remembering fine details of the call.

• The threat recipient should keep the caller on the line as long as possible. The recipient should ask what type of device it is, what it looks like, why the caller placed the bomb, who the caller is, etc. The caller should be advised that the building is occupied and that a deto-

nation may result in the death or injury of innocent people. The objective is to gain as much information as possible about the caller and the credibility of the threat. If the recipient doesn't know what to ask, he/she should refer to the card for a list of questions.

• While listening to the caller, the recipient should pay attention to noises in the background, the sound of the caller's voice, his/her use of idiom, and any other indications of the caller's identity or the source of the call.

• After the caller hangs up, the recipient should immediately report the situation to the incident commander or a security officer. Before speaking with anyone else, the recipient should complete the questions on the bomb threat card. This ensures documentation of the threat while everything is fresh in the recipient's mind.

Step Three: Determine a procedure for evaluating threats.

At this stage, a procedure needs to be established for evaluating threats and deciding on the next course of action.

Once the threat call is received and security is notified, the incident commander should debrief the person who received the call. Before asking any questions, the incident commander should let the person who received the call describe the conversation in his/her own words. This ensures that the recipient is speaking directly from memory without the influence of outside suggestions. After he/she has finished the account, the incident commander should review the completed bomb threat card to ensure that the person recorded every detail to the best of his/her ability.

Determining the authenticity of a bomb threat is a very difficult task. In most cases, the statements of the caller alone are insufficient to enable a clear determination. However, there are some characteristics that may indicate an authentic threat. Many authentic bomb threat callers will repeat their message in a very specific and deliberate manner. In this situation, the bomber wants to be sure that the message is accurately understood. In other cases, the bomber may reveal the location of the device. Detailed descriptions about the location of the device or how the device is constructed are strong indi-

Bomb Threat Card

Questions to ask:

1.When is the bomb going to explode?

2.Where is it right now?

3.What does the bomb look like?

4.What kind of bomb is it?

5.What will cause it to explode?

6.Why did you place the bomb?

7.What is your name?

Exact wording of the threat:

_____

_____

_____

_____

_____

_____

Details of the call:

Sound of the caller's voice: _____

_____

_____

Background noises/sounds:_____

_____

_____

_____

cations that the threat is authentic. Generally, the more information provided by the caller, the greater the chances are that the call is real.

In some parts of the world, terrorist groups use coded warnings to verify the authenticity of bomb threats. In this situation, the caller states a code word while delivering the bomb threat. The police, once notified, understand what the code word means. While most coded warnings are called directly to police or news media organizations, coded warnings may be delivered directly to the threatened facility.

At this stage, a decision needs to be made about whether to evacuate, search, or ignore the threat. This decision should be made according to standard protocol as defined in the bomb threat plan. For example, a policy might be established stating that a search of the facility by employees will be initiated immediately after a threat is received—regardless of the circumstances of the call. In other situations, immediate evacuation and a full search by trained search teams should be conducted.

At most chemical facilities, a mandatory employee work area search will be the best choice as first step.

A note about threat credibility indicators

Do not base the decision to search or evacuate solely on the appearance of the threat call's credibility. Many authentic callers do not provide definitive indications that a threat is credible. Guidelines for principal decisions about search and evacuation should be established as standard policies during the initial planning process.

So what is the value of assessing potential threat credibility?

Strong indications of threat authenticity are often useful when deciding what to do once a search or evacuation is complete. For example, what if a search is conducted and nothing is found? Should the building be evacuated or reoccupied before the time stated in the threat call? If the threat appeared credible, a decision to evacuate or postpone reoccupation until after the stated time may be justified. It is possible that the search teams did not locate the bomb.

Step Four: Determine an Incident Command Point (ICP)

Once the threat response plan is initiated, the incident commander should move control operations to an incident command point (ICP). The location of the incident command point will depend on the type of search and response plan initiated. For example, if an employee work area search is initiated, the ICP should be located at an office close to the entrance or close to the exterior of the facility. If an evacuation is required, the ICP would then relocate to an alternate position outdoors (such as a security gate shack).

To ensure that the ICP is ready to move and set up quickly, all items needed to control search and response activities should be located together in a portable ICP kit. This should contain a copy of the bomb threat response plan, a copy of the facility layout (marked with evacuation routes and search zones), emergency telephone numbers, staff rosters, internal extension numbers, etc). The ICP kit should also include any equipment necessary to conduct the search, such as flashlights, duct tape (for marking areas that have been searched), and rope and hooks.

Step Five: Develop a search and evacuation plan.

The search and evacuation plan should detail the steps taken immediately after receipt of the bomb threat. The plan should also provide guidelines for making critical decisions such as when to evacuate and reoccupy the facility.

Three primary methods are used for search and evacuation in response to bomb threats:

1. Security Team Search
2. Employee Work Area Search
3. Police Assisted Search

Part 2 of this article continues with an examination of search and evacuation protocols and response procedures. To view this article in its entirety, request a free copy of the Chemical Plant Bomb Threat Planning Handbook by sending an email to: chemical_security@cisworldservices.org.

Vehicle Search Procedures

By Craig S. Gundry, CPS
Vice President of Special Projects, Critical Intervention Services

To minimize the risk of deceptive and naive vehicle bomb deliveries at high risk chemical facilities, security personnel may be required to physically search vehicles as a supplement to other access control practices. Unfortunately, as our consulting team has witnessed at a number of chemical sites, many facilities that have implemented vehicle searches are using ineffective search procedures or have provided little, if any, training to site security personnel. The procedure outlined in this article is provided as a model for facilities that wish to improve their existing search protocols.

The method of search that we recommend requires two guards to conduct the search. One guard physically searches the vehicle while the second guard carefully observes the driver and occupants for any signs of suspicious behavior or anxiety. For maximum effectiveness, a checklist should be used to ensure that the search is conducted properly and documented.

Step One: Prepare the vehicle for search.

As a vehicle is identified for search, the driver should be instructed to park the vehicle in the search area, turn off the engine, retrieve the logbook, and step out. Any passengers should also be instructed to exit the vehicle. The first guard should then examine the logbook for any inconsistencies. Is the logbook up-to-date? The guard should question the driver about the last few entries while observing the driver's behavior for signs of anxiety. An incomplete logbook or a driver that cannot answer simple questions about previous entries should be automatically regarded as suspicious.

Next, the guard leading the search should instruct the driver to open all doors, the hood, and the trunk. If the vehicle is a truck, the driver should also open the back of the cab or trailer.

While the first guard is inspecting the vehicle, the second guard should carefully watch the driver and passengers for any signs of increased anxiety or agitation. The second guard should be prepared to use force in the event that a bomber panics and attempts to activate the device.

Step Two: Search the passenger compartment.

Next, the first guard should inspect the passenger area. If there are any jackets or objects concealing view of the seats or floor, the guard should instruct the driver to remove these items. Without touching anything, the guard should carefully observe any unusual wires or cord running through the interior, small boxes or enclosures with wires extending to another part of the vehicle (possible control or arming devices), signs of tampering along the edges of seats and dashboards, and any large boxes or containers.

Step Three: Search the exterior of the vehicle.

Inspect the exterior of the vehicle for any suspicious characteristics. Begin near the front of the vehicle and work around the back and the opposite side.

If the vehicle is a truck, carefully observe the gas tanks for any signs of repair, welding, or new paint. Tap the top and bottom of the tank. Notice if the bottom sounds hollow while the top sounds full. Bombers have used false compartments in gas tanks to conceal explosive charges on a number of occasions.

The area between the truck cab and the trailer should also be carefully inspected. Notice any wires or lengths of cord connecting the cab and the trailer. Many bombers conceal the activation system or arming features in the cab while running a length of wire or detonating cord to the rear cargo area. Any pairs of thin single-conductor wires or plastic or textile-covered cord should be reason for suspicion—particularly if the wires or cord appear brown, olive, or brightly colored.

While moving around the vehicle, the guard should be aware of any unusual scents of petroleum products or acidic smells (such as burning time fuse). The rapid

onset of a headache during the search is another reason for suspicion. Two explosives with high vapor pressure (nitroglycerin and methyl nitrate) often produce headaches when their vapor is inhaled.

If the vehicle is a tanker truck, the area around the tank should be closely inspected for any unusual objects in close proximity. Particularly note any objects affixed to the tank itself, wires connecting unusual objects to other areas around the vehicle, and any items that resemble communications equipment (such as pagers, cell phones, radios, or model aircraft/car parts). This inspection should include the top and bottom of the tanks as well. As demonstrated in the May 2002 bombing at the Pi Glilot petroleum and gas facility in Israel, terrorists may attempt to conceal a device on a vehicle operated by an innocent driver. This type of naïve delivery at a chemical plant would most likely employ a truck carrying combustible or explosive cargo (relying on the secondary explosion to damage on-site facilities and equipment).

When the back of the vehicle is inspected, the license plates should be compared with the logbook and registration to ensure that they match. If the vehicle is a truck or box van, the guard should also examine the rear bumper or trailer step for signs of fresh rust. Many improvised explosives employed in vehicle bomb attacks use corrosive oxidizers. While building the bomb, some of this explosive may leak or be swept onto the bumper, leaving patches or spots of fresh rust.

Many security managers instruct personnel to search the underside of entering vehicles using inspection mirrors. In most entry point situations, this is a waste of resources. With the possible exception of a tanker truck as a naïve delivery vehicle, devices mounted underneath a vehicle are planted to target the vehicle or its occupants—not the facility to which it is traveling.

Step Four: Inspect the trunk or cargo area.

The guard should pay close attention when inspecting the trunk or cargo area. These are the most common locations for concealing the main explosive charge. In most vehicle bombs, the main charge is concealed in one or more large containers. Many explosives commonly used in large bombs (e.g., ANFO, urea nitrate, etc.) require a sealed container, such as a bag, barrel, or drum. Other explosives, such as dynamites, may be stored in their original cartons or repacked into boxes. Placement of these containers is usually positioned in the forward part of the truck's cargo area or car trunk.

If multiple containers are used for the main charge, wires or lengths of detonating cord may be visible connecting the charges together. Many explosives used in vehicle bombs require a booster for initiation. This may be visible as a brightly colored cylinder or (more likely) as a typical high explosive charge or small container filled with explosive.

If the vehicle is a cargo truck, the guard should physically enter the back and inspect the entire interior of the cargo area including the areas behind any palettes or tarps. Terrorists often stack objects in front of the main charge to conceal it from casual view. The Provisional Irish Republican Army, for example, would often place a board in front of the explosive charge to conceal it from view at the rear of the truck.

During the search, the second guard should continue to watch the driver and passengers. If at any point during the search, the driver or passengers demonstrate signs of increased nervousness, this may be an indication that the first guard is close to the location of something concealed. If this is observed, the subjects should be walked away from the vehicle while the first guard intensifies his search of that area.

Step Six: Release the vehicle and document results.

Once the back of the vehicle is inspected, the driver should close up the vehicle and proceed to his/her destination inside the facility. The vehicle's inspection should be noted in the facility’s access control log.

If at any point in the search, something suspicious is observed: stop immediately! The second guard should hold the driver and passengers in custody while the first officer alerts the security department or police. The area around the vehicle control point should be evacuated while the security department initiates the facility response procedure.

For additional assistance regarding vehicle access control planning or security training, contact Critical Intervention Services at (727) 461-9417 or send us an email: chemical_security@cisworldservices.org.

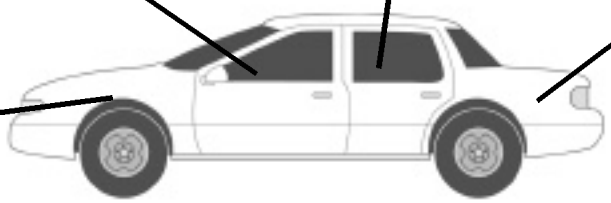
POTENTIAL VEHICLE BOMB INDICATORS

Interior (Front Seat Area)
Unusual boxes or switches, wires or cord extending to other parts of the vehicle, jackets concealing objects from view, signs of disassembly/ reassembly along dashboard and upholstery

Interior (Back Seat Area)
Unusual wires, cord, visible explosives, boxes, bags, gas cylinders, signs of repaired upholstery

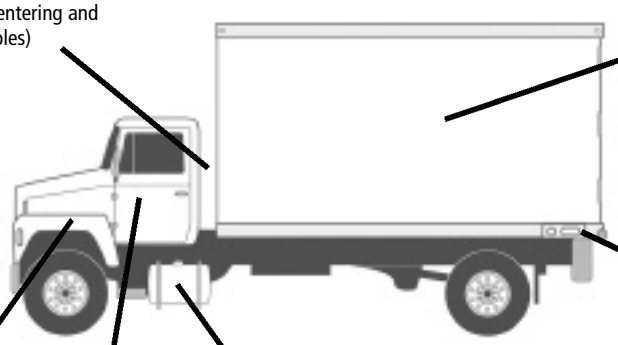
Trunk (Inside)
Unusual wires, cord, visible explosives, boxes, bags, or gas cylinders

Engine Compartment
Unusual wires or cord extending to other parts of the vehicle



Area between Cab and Trailer
Unusual wires or cord connecting the cab and trailer (possibly entering and exiting through drilled holes)

Cargo Trailer (Interior)
Unusual wires, cord, visible explosives, boxes, bags, drums, barrels, gas cylinders (particularly any assembly involving multiple containers connected together by cord or wires)



Rear Trailer Step & Base of Trailer
Signs of fresh rust (particularly isolated patches of bright rust or shoeprint-shaped rust spots)

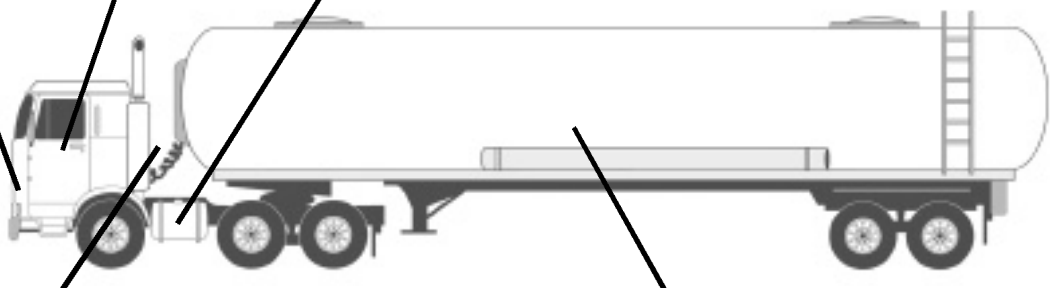
Engine Compartment
Unusual wires or cord extending to other parts of the vehicle

Cab (Interior)
Unusual boxes or switches, wires or cord extending to other parts of the vehicle, jackets concealing objects from view, signs of disassembly/reassembly along dashboard and upholstery, unusual drilled holes with wires or cord exiting the cab

Gas Tanks
Signs of repair or new installation, hollow bottom/full top

Other Threat Indicators:

- Unusual odors
- Intense "headache" while moving around the vehicle
- Nervous or unusual driver behavior
- Driver lacks familiarity with log book entries
- License plates do not match registration or log book



Area between Cab and Trailer
Unusual wires or cord connecting the cab and trailer (possibly entering and exiting through drilled holes)

Tank Trailer (Exterior)
Unusual objects attached to tank,unusual wires or cord connecting objects to other parts of the vehicle, any object that resembles communications equipment (radios, pagers, etc.)

Upcoming Events

DATES	EVENT / LOCATION	HOST
10/28/02-10/29/02	**Assessing Terrorism-Related Risk Seminar** Clearwater, Florida	S2 Safety & Intelligence Institute www.s2institute.com / Tel.(727) 461-0066
11/6/02-11/7/02	**AIChE Security Vulnerability Assessment Course** Indianapolis, MN	Center for Chemical Process Safety AIChE Education Services, Tel.(212) 591-7526
11/14/02-11/15/02	**AIChE Security Vulnerability Assessment Course** Las Vegas, NV	Center for Chemical Process Safety AIChE Education Services, Tel. (212) 591-7526
12/9/02-12/10/02	**AIChE Security Vulnerability Assessment Course** Jacksonville, FL	Center for Chemical Process Safety AIChE Education Services, Tel.(212) 591-7526
12/9/02-12/10/02	**Anti-Terrorism Officer Course** Clearwater, Florida	S2 Safety & Intelligence Institute www.s2institute.com / Tel.(727) 461-0066