RESERVOIRS

BusinesSafe is based on the idea that certain businesses and industries may be exploited by terrorists who portray themselves as honest customers seeking to purchase, lease or somehow appropriate certain materials, licenses and/or services to covertly further a terrorist plot.

The following are general indicators of potential terrorist planning or activities. Alone, each indicator can result from legitimate recreational or commercial activities or criminal activity not related to terrorism; however, multiple indicators combined with other information may possibly suggest a terrorist threat.

- Physical surveillance, which may include note taking or the use of binoculars, cameras or maps near key facilities.
- Attempts to gain sensitive information regarding key facilities or personnel through personal contact or by telephone, mail or e-mail.
- Attempts to penetrate or test physical security and response procedures at key facilities.
- Attempts to improperly acquire explosives, weapons, ammunition, dangerous chemicals, flight manuals or other materials which could be used in a terrorist attack.
- Suspicious or improper attempts to acquire official vehicles, uniforms, badges, access cards or identification for key facilities.
- Presence of individuals who do not appear to belong in the workplace, business establishment or near a key facility.
- Behavior which appears to denote planning for terrorist activity, such as mapping out routes, playing out scenarios, monitoring key facilities and timing traffic flow or signals.
- Stockpiling suspicious materials or abandoning potential containers for explosives (e.g., vehicles or suitcases).

The following examples of activity relating to Reservoirs, though not fully inclusive, may be of ***possible*** concern to law enforcement, as well as this sector:

- Large size reservoirs (perimeters that often exceed 20 miles in length).
- Readily available access routes and facility maps.
- Sufficient cover to hide the activities of an adversary.
- Multiple uses that promote recreational activities and visitors.
- Critical facilities or assets not completely or adequately enclosed.
- Gates and critical assets near the perimeter fence line or on the site not protected by appropriate barriers or other hardening equipment.
- Facilities located in remote, rural, or semi-rural locations.

- Public roads or rail lines that pass through, pass over, or adjacent to some sites, making it difficult to protect the perimeter. Sites adjacent to waterways make it more difficult to control access.
- Sites without rigorous procedures for inspecting vehicles for explosives and/or dangerous materials before they enter the facility or to escort them after they enter the facility.
- Facilities that use contract guard services. There may be variability in the background checks, training, and equipment available to the guard force. Turnover rates in the guard force may be high.
- Facilities without signs posted to deter vehicles, boats, or pedestrians from entering unauthorized portions of the facility.
- Camera surveillance that does not cover all critical assets.
- Inadequate lighting in certain parts of the facility (e.g., too little, poorly spaced, or improperly directed).
- Entrances to critical assets within the facility (e.g., control rooms) without controlled access. Once someone has gained access to the site, that individual potentially could access multiple areas within the facility.
- Facilities in which access identification that is not required or adequately enforced.
- Employee and visitor parking located next to critical buildings.
- Facilities where background checks conducted on employees, vendors, and contractor personnel are limited. Some states or even union contracts limit the use of background investigations.
- Know coordination gaps with local, state, and federal agencies on roles and responsibilities.
- Web sites providing detailed information on facility locations, critical assets, maps, and other operational data.
- Computer hacking: this activity might provide adversaries with additional information.
- Standardized systems (e.g., Windows) and protocols used for process control systems such that a vulnerability exploited at one facility may be relevant at multiple facilities.
- Lists of facility locations available through public sources.
- Lack of security around servers and control rooms: Intruders could potentially hack into process control computers through the company enterprise network.
- The facility may not maintain a backup control center: Backup facilities may not be in place for the Emergency Operations Center.
- Fires or explosions: This may present difficult challenges to first responders. Additional coordination of emergency plans may be needed with facility neighbors and with local, state, and federal government authorities.
- Loss of electric power that might significantly disrupt facility operations and create significant public safety conditions.
- Electric power equipment (e.g., transformers, transmission, distribution lines, and substations) that provides service to the facility that might be readily identified and unprotected.

- Multiple organizations involved in providing electric service to a facility that have different degrees of security.
- Loss of natural gas that reduces or shuts down facility operations.
- Although most natural gas pipelines are underground, valves, and other aboveground equipment may be visible and detectable.
- Signs that are used to identify right-of-ways for natural gas.
- Contamination or loss of water supply that reduces or shuts down facility operations. Be aware of water supplies that may be received from a single pipeline: this may inhibit firefighting capabilities.
- Spare parts that are large and/or expensive might be in short supply (e.g., water pumps). Economic considerations may have reduced these spare-part inventories. Some parts have long lead times to obtain or are available only from overseas vendors.
- Telecommunications may rely on the public-switched network: telephone congestion, including land lines and wireless, may occur during emergencies.
- Disruption of communications could reduce or shut down a facility. Therefore, handheld radios may be critical to facility operations.
- Adversaries that might scan communication frequencies to determine operating conditions, location of employees, on-going activities, etc: communication with first responders is crucial to react in a timely manner to incidents. Jamming or other methods may be used to disrupt communication channels.
- Loss or disruption of different transportation systems vital to the facility, including road, rail, or waterway. Disruptions to the transportation system may inhibit effective implementation of emergency procedures (e.g., evacuation, emergency response)
- Loss of operations at one facility that cascades and results in loss of operations at nearby or related facilities.

Your impressions and assessment based upon your professional business experience are extremely valuable and should help guide you in determining if a customer request, a fact pattern, or set of circumstances is unusual.

Please remember that the conduct of an individual will not necessarily be criminal in nature. Suspicious incidents should be reported immediately to your local law enforcement agency, Crime Stoppers, or your regional FDLE office. You may also email a tip regarding a suspicious incident utilizing the link on the BusinesSafe homepage.

For all emergencies, call “911.”