DAMS

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 Dams, though not fully inclusive, may be of ***possible*** concern to law enforcement, as well as this sector:

- Public roads that are close to the facility that provide easy access to and escape from the facility.
- Critical facilities or assets that may not be completely or adequately enclosed.
- Critical assets that are near the perimeter fence.
- Gates and critical assets near the perimeter fence line or on the site that may not be protected by appropriate barriers or other hardening equipment.
- Facilities that are located in remote, rural, or semi-rural locations.
- Public roads or rail lines that pass through, over, or adjacent to a Dam.

- Sites that do not have rigorous procedures to inspect vehicles, or they may not have adequate vehicles to escort them once they enter the facility.
- Contract guard services because of the variability in background checks, training, and equipment. Be aware of turnover rates in the guard force that are high.
- Facilities that do not have signs posted to deter vehicles, boats, or pedestrians from entering unauthorized portions of the facility's premises.
- Camera surveillance that does not cover all critical assets.
- Lighting that is inadequate in certain parts of the facility (e.g., too little, poorly spaced, improperly directed).
- Entrances to critical assets within the facility (e.g., control rooms) that do not have controlled access.
- Identification for access that is not required or adequately enforced.
- Employee and visitor parking that is located next to critical buildings.
- Limited background checks conducted on employees, vendors, and contractor personnel,
- Gaps that may exist in the coordination of roles and responsibilities with local, state, and federal agencies.
- Websites that may provide detailed information on facility locations, critical assets, maps, and other operational data.
- Lists of facility locations that may be available through public sources.
- The lack of security around servers and control rooms.
- There is a potential for intruders to hack into process control computers through the company enterprise network.
- There is a potential for a process controller to cause an undesirable event.
- Standardized systems (e.g., Windows) and protocols that could be used for process control systems wherein a vulnerability exploited at one facility may be relevant at multiple facilities.
- Contingency plans that may not be exercised on a routine basis.
- Facilities that do not have emergency operation center backup facilities.
- Loss of electric power that may significantly disrupt facility operations and/or create significant public safety conditions.
- Electric power equipment (e.g., transformers, transmission and distribution lines, substations) that provide service to the facility may be readily identified and unprotected.
- Multiple organizations that provide electric service to a facility and have different degrees of security.
- Telecommunications that rely on the public switched network.
- Facilities that do not have handheld radios in the event of an incident.
- Communication frequencies might be scanned to determine, for example, operating conditions, the location of employees, and ongoing activities.
- Loss of operation at one facility that may cascade and result 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.”