BUSINESSAFE

COMMUNITY WATER FACILITIES

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

- Water service directly provided to private areas (e.g., houses or commercial buildings).
- Understaffed security departments for municipally-owned facilities.
- Accessible wells that may be vulnerable.
- Valves that connect water facilities are accessible.
- Systems that chlorinate, but do not use filtration or other water treatment.
- Lists of water supply facility locations available through public sources.
- Disgruntled employees that have knowledge of and access to vulnerable locations or the ability to alter data or algorithms used to control the system.
- Servers and control rooms that lack security.

- Cyber Attacks: increased use of informational management systems that cause potential vulnerabilities to the water system and potential for intruders to hack into SCADA process control through an enterprise network. NOTE: SCADA is an acronym that stands for Supervisory Control and Data Acquisition.
- SCADA systems that use the telecommunication network to communicate between sensors and control rooms, to provide information to maintenance and management personnel, and to provide data needed for accurate billing to customers. These systems need to be closely monitored.
- Large quantities of chlorine or similar disinfectants stored on site for water purification and chemical processing.
- Large storage tanks easily identifiable from off site.
- Toxic chemicals that pose serious scenarios, if released.
- Damage to critical assets, treatment plant processes, or pumping facilities that could interfere with the utility's capability to produce safe, pressurized water for consumption, firefighting, and other uses.
- Water pipeline right-of-ways that are shared with natural gas pipelines or other utilities.
- Maintenance and repair of water system components that may require the movement of personnel, equipment, and heavy-duty vehicles (e.g., cranes) over distances can be significant.
- Maintenance and repair of water systems that may require streets or roads to be torn up and then repaired.
- Disruption to the Transportation Sector; access to facilities, deliveries of treatment chemicals and other supplies, waste disposal, and other operational functions.
- Water pipelines that are be co-located with underground electric lines or on the same right-of-ways as overhead lines.
- Restoration of water service that may be of lower priority than restoring electric power. In some cases, repairs to the electric system must be completed first to provide power to repair the wastewater system.
- Loss of electric power that impact the ability of water treatment facilities to produce water for the electric, natural gas, and oil industry. Water is used by these industries for production, cooling, and emissions reduction.
- Water utilities that lack sufficient backup generating power to meet their needs during an extended loss of electrical power.
- Disruption of communications that delay notification of an incident and/or increase the response time. Handheld radios may be critical in responding to wastewater system emergencies.
- Wastewater systems that rely on remote sensors to measure water flow, pressure, quality, and other operational parameters. Disrupting or altering the data from these remote sensors may result in the addition of incorrect chemicals, over-pressurization of the pipelines, or other disruptions, or it may cause an existing disruption to go undetected.

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.”