



WASTEWATER TREATMENT FACILITIES

BusinessSafe 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 Wastewater Treatment Facilities, though not fully inclusive, may be of **possible** concern to law enforcement:

- Theft or unexplained loss of chemicals from your business inventory, tractor-trailer or treatment facility.
- Unusual inquiries from strangers concerning how your treatment facility stores chemicals or handles them on premises. Similar or other inquiries from a previous customer whose identity is not clear.
- Apparent surveillance of your facility or business by unknown persons.
- Apparent surveillance of one or more of the chemical feed points within the treatment facility.
- Any observed alterations to flow-paced chemical injection equipment.

- Unusual or suspicious deliveries or substitutions of the wrong treatment chemical.
- Deliveries, driver identification, companies do not mirror the company to which chemicals were purchased from. Interviews and manuals of terrorists have indicated the possibility of poisoning the water during the water treatment process. They have mentioned inserting a poison into the chlorination section of the water treatment facility.

Proactive measures of the facility are recommended:

- Perform a thorough check of credentials provided by current and new employees.
- Ensure that any suspected disgruntled employees or former employees do not have unescorted or unsupervised access to chemical injection or additional points within the treatment facility or wells.
- Pay particular attention to contractors and vendors. Do not allow unescorted access to critical areas of the treatment facility by any contractor or vendor.
- Verify that access to remote chemical addition points is secured.
- Ensure that chemical injection points or chemical addition areas within the treatment facility are closely monitored. Do not allow unauthorized personnel access to these critical areas.
- Maintain extremely high accountability of all concentrated hydrogen peroxide stored at water treatment plants
- Ensure that the SCADA terminals and systems have alarms for overfeeding and are only accessible by authorized personnel.
- Ensure compliance with best practices Cyber Security Standards such as those issued in 2019 by the North American Electric Reliability Council.
- Certify that the facility has a chemical delivery integrity program and “know your suppliers and vendors.”

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.”