



## CRITICAL MANUFACTURING

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

- Individual(s) videotaping, photographing, or sketching the premises for no apparent reason.
- Apparent surveillance of your facility or business by unknown persons monitoring the arrival, departure, and/or frequency of delivery trucks.
- Unusual or suspicious deliveries or substitutions.
- Suspicious inquiries concerning utilities servicing the facility.
- Suspicious vehicles parked in proximity to your facilities.
- Reports of unknown persons observed trespassing on your property or taking photographs of your facility or equipment.

- Reports by employees of being questioned by suspicious individuals as to their routine or activities.
- Individual(s) found in areas restricted to only site staff and not open to the general public.
- Attempts to gain employment at sensitive sites or outside vendors offering access to these sites.
- Applications to your company for employment by individual(s) who submit identification documents of questionable authenticity (i.e., home address is represented as a P.O. Box; no telephone number; misspellings on "official documents"; different names on license and passport).
- Unusual questions about the type of security in place at your facility.
- Inquiries regarding the frequency of maintenance, storage, and usage of supplies and equipment.
- Any requests for information involving operational safeguards of suppliers, purchasers, transporters, of products etc.
- The discovery of an unattended package or object inside or around the facility.
- Individuals who allege to be a waste removal or clean-up contractors and are willing to remove your used or unused waste from your inventory for an unusually low nominal fee or free of charge.
- Deliveries, driver identification, or company name or identification that do not appear to correlate with the company they were purchased from.
- The registration or inspection sticker on the deliveries appear altered or fraudulent.
- Reports of individuals attempting to make unscheduled deliveries or "complimentary" maintenance visits.
- Individuals bringing or attempting to bring unusual packages or containers into the premises.
- Overheard conversations in which individuals make unusual or alarming statements.
- Maintenance work that is not announced or scheduled takes place.
- Evidence suggesting that the building's HVAC system (i.e., heating, ventilation, air conditioning access rooms or panels) may possibly have been tampered with.
- Transaction(s) involving an intermediary agent and/or third party consignee that is unusual in light of their usual business.
- Unusual customer request concerning the shipment or labeling of goods.
- Unusual customer request for excessive confidentiality regarding the final destination or details of the product to be delivered.
- A customer who cancelled a sale, and coincidentally the exact same product is stolen or "lost" shortly after the customer's inquiry.
- Theft or unexplained loss of equipment or supplies.
- Theft or loss of entry keys or identification passes/badges that furnish access or allow access to the premises.
- The unexplained loss, theft, or attempted theft of equipment or individual machine components used in your manufacturing.

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 [BusinessSafe homepage](#).

For all emergencies, call "911."