INFORMATION TECHNOLOGY – CYBER SECURITY

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

- Unexpected deliveries or complimentary software.
- Individual(s) videotaping or photographing your facility.
- Any reports of unknown persons trespassing on the property.
- Maintenance work that is not announced or scheduled.
- Loss or theft of an employee’s identification badge or keys.
- Loss or theft of computers or electronic equipment.
- The loss or theft of information from your system.
- Any apparent break-ins or tampering with the system (i.e. the discovery of key stroke recording device).

- Unusual inquiries from individuals regarding cyber security at you company/agency/entity.
- Unusual requests on how to clean computers or erase the electronic path or trace of its user such as wiping software, anonymous browsing software, etc.
- Unusually excessive or suspicious telephone activity at your facility.
- Unusual inquiries regarding applications of the system, software used, and protective security.
- Inquiries regarding the frequency of maintenance, time of security checks, and security patrols, etc.
- Suspicious inquiries regarding utility service to your facility.

Some suggested protective security measures include:

- Authenticate and maintain authorized users of your cyber system.
- Securing all of your wireless networks.
- Removing all information from the equipment before disposing of it.
- Improve the security of your outsourced work by checking credentials.
- Participate in information sharing and analysis centers and information technology security programs with your state and local government.
- Continuously assess threats and vulnerability to your cyber system.

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.”