ELECTRONIC SHOPS, SPY SHOPS, COMPUTER STORES AND SUPPLY, AND INTERNET CAFES

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 Electronic Shops, Spy Shops, Computer Stores & Suppliers, and Internet Cafes, though not fully inclusive, may be of ***possible*** concern to law enforcement:

- Loss or theft of computer or electronic equipment pertaining to surveillance such as night-vision goggles, special use binoculars; items that may be utilized as bomb making components such as wirers, digital timers, electronic relays; encryption or steganography software, or any other unusual software or equipment.
- Specific requests of employees regarding eavesdropping devices, equipment to surreptitiously duplicate documents, or unusual counter-surveillance equipment from an individual(s) that would not have an apparent legitimate need.

- Any unusual request for information or procedure relating to how to clean computers or erase the electronic path or trace of its user such as wiping software, anonymous browsing software, etc.
- Purchase of expensive photography or video equipment with panoramic capability.

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.”