



## Ten Security Procedures That Will Help to Deter or Mitigate Terror Attacks

- 1. Enforce a Standoff Zone:** A standoff zone is a secure area in which only pre-screened vehicles, bicycles, etc. are allowed to enter. A 100' to 300' standoff zone is ideal, but the effects from a blast are decreased in direct correlation to the increase in distance between a blast and its intended target. Therefore, even a 10' standoff zone is better than no standoff zone. Bollards, barriers and barricades (natural and man-made) are used to enforce the integrity of the standoff zone.
- 2. Implement Surveillance Detection:** Nearly every major terrorist attack has been preceded by months and years of surveillance. Initial surveillance is usually conducted by amateurs or unwitting accomplices (children, taxi drivers, delivery/service persons, etc.) paid to take photographs, provide facility descriptions or other information (or information is surreptitiously elicited from them). Once a target list is narrowed, comprehensive surveillance is conducted by "professional" operators. Security personnel should be trained to observe and report unusual interest in a facility or activities that are out of context for the environment (e.g. taxi driver photographing a service entrance). As planning progresses, operators may conduct tests or dry runs, such as attempting to enter a restricted door to test the security response, or driving the intended route to identify potential obstacles.
- 3. Screen Deliveries:** All delivery, service and courier vehicles and their contents should be screened using the following procedures: a) deliveries, other than courier services, should be scheduled in advance, and drivers should be required to present a bill of lading that reflects the driver's name and a password issued by the Receiving Department, b) all drivers, including couriers, and their assistants should present photo identification and their presence should be documented, c) all license tags should be documented, d) ideally, cargo areas will be inspected by security at a remote location and sealed by security until arrival in the receiving area, where the seal will be broken by building security or a receiving clerk/dock master, e) all incoming parcels should be x-rayed or physically inspected, and f) no parcels should be accepted anywhere other than at the designated receiving area.
- 4. Stagger Security:** The numbers of security personnel on-duty, as well as the times at which shifts change, should vary by day to eliminate a discernable pattern. When conducting patrols, security personnel should use random start and finish times and vary their routes (at times, even suddenly changing direction or backtracking). If possible, vary the methods of patrol (vehicle, bicycle, walking). The use of both uniformed and "plain clothed" security personnel is advantageous.

5. **Facilitate Evacuation:** During non-business hours, facility management personnel should conduct an evacuation drill using only emergency lighting in the emergency exit stairways. This enables them to mimic, as closely as possible, a real life emergency scenario. Often, these “evacuees” identify critical hindrances in stairways, such as: a) the need for additional emergency lighting on each landing; b) the benefit of luminous paint, decals and/or signs, at floor and eye levels, to highlight primary and secondary escape routes; and c) the need for public address speakers in the stairways, so evacuees can hear important announcements. Where possible, stairways should be widened, and separate stairways should be provided for exclusive use by emergency personnel. (Evacuees often block access by firefighters.) Stairways should never exit into public lobbies.
6. **Screen Visitors:** Where possible, screen visitors at a remote location, distant from any facilities. Visitors should be scheduled, in advance, by their hosts, and hosts should be required to escorts visitors at all times. Visitors should present government-issued photo identifications, which should be held until their visitors’ passes are returned. (This is known as a credential-exchange program.) Hand-carried belongings should be visually inspected or x-rayed, and persons should be required to pass through a magnetometer. Outerwear, such as jackets and coats, should be opened and/or removed for inspection.
7. **Screen Employees:** All employees should be required to wear facility-issued photo identification at eye level on their outermost garments. The use of access cards is recommended, and is best when used in conjunction with biometric or keypad systems. Always verify either electronically or visually that the card holder is the person to whom the card is issued; and never assume that an employee with whom you are acquainted is still employed at the facility.
8. **Review Your Emergency Procedures:** Know what to do and when to do it. Review, and if necessary, update your security, evacuation and life safety procedures and policies.
9. **Make Security the Responsibility of All Users:** Everyone that works at your facility should be reminded continuously to observe and report unusual behavior. Users should politely challenge those who appear lost or are not known to them. Simply acknowledging them and removing their anonymity might deter a potential incident.
10. **Assess Your Security:** Retain a security consultant to assess your physical, technical and operational security. Where possible, their involvement early in the architectural, engineering, landscape design and construction phases can help to avoid costly rectification later. Experts that are Board Certified in Security Management (CPP) and Board Certified in Physical Security (PSP) can best manage the complexity of regulatory, legislative and best practices changes, and use them to guide their recommendations. Importantly, security consultants must be independent of affiliation with any product or service, thus ensuring that the services they render are in the best interests of the client.

