PBIED

Definition: A suicide attack in which the attacker(s) wear or carry an improvised explosive device.

Access Control

Public/Non Public Control: This will include all other methods of access control not covered by guarding and search and screening. This will include reception staff, ticket check staff, electronic and mechanical access control, signage and key control.

Full Time Operational Access Control Policy/Process: This will detail the policy and process to deal with unauthorised access response, removal of ex staff members from electronic databases, dealing with lost keys etc.

Dynamic Lock Down Policy: Can the site lockdown and be secured quickly in response to a direct or proximity threat/attack.

Training/Awareness

Deterrence Tool Kit: We have developed a set of back of house communication materials, based on the security infrastructure, which cause concern to terrorists about being detected. The materials achieve this in two ways: creating the impression that the site knows what hostile reconnaissance is (what they are up to), and that everyone is watching out for them. Details can be provided by your CTSA.

IED

Definition: An improvised explosive device that is placed or secreted at a site. The device may be carried in any type of container, such as a bag or rucksack, so as not to stand out and to avoid detection.

Guarding

Active Search Regime: This is deterrent and detection activity. Examples would include regular inspection of bins, foliage and toilets. Should include all areas and spaces where IED could be left/placed.

Security Planning

Housekeeping: These are the good practice processes to deter or detect placed IED's. Examples to be included in the policy include foliage to be regularly trimmed, regular emptying of bins, staff to conduct pre-opening and post-closing searching of premises.