CORPS
CONSULT

ICONIC & HIGH-RISK SITES/PREMISES

Resilience & Security Guidance

Date of Issue: November 2018

1. Introduction

- This guidance document is intended to be used by those responsible for resilience and security at iconic and high risk premises and facilities. The contents of this guide do not provide site-specific solutions, but are intended as generic guidance on how to set about formulating site specific security plans and resources
- Readers and users of this guide are advised to set about securing their relevant premises and facilities by reference to site specific security risk and threat assessments, which should be conducted by appropriately qualified security professionals
- *'Corps Consult Security Ethos':*
- Our general approach and methodology to delivering security solutions is underpinned by our adherence to our unique 'Eight Principles of Security' which are described as follows:

1. Clearly defined security policy
2. Intelligence & Information

3. Manpower & Human Resources
4. Technical Means
5. Operational Procedures
6. Control & Supervision
7. Tests & Drills
8. Internal and External Security Audit

Principle No 1: The first of these is to define a policy and strategy. This should contain all assessed risks and threats and be endorsed at board level. Not only will this ensure that it is fully supported, it will also mean that an appropriate financial budget is allocated to carry out any necessary measures.

Principle No2: The next is to implement an information and intelligence gathering process to clarify the requirements. For example, an organisation that is moving premises should examine local crime trends and statistics in its new location, look at other building occupiers in the vicinity and assess whether they pose any direct or indirect dangers.

Principle No 3: The third principle reflects the fact that human resources, i.e. people, are the most important facet of any security programme. Human intervention is essential and trained personnel, whether specialist technical operators, security officers or other employees who have undergone security awareness training, are the eyes and ears of corporate security.

Principle No 4: This principle addresses an organisation's technical means. The astonishing advances in technology have brought significant benefits to the way security solutions are configured. To be effective most strategies will utilise a combination of technology and human resources, including the use of remote monitoring and other electronic assets.

Principle No 5: This principle defines the control and supervision methods needed to manage the policy and strategy. Any confusion surrounding this issue can be positively dangerous, especially during the management of a crisis or contingency.

Principle No 6: Every security programme will require appropriate operating procedures, in order to achieve optimum and safe results. Even the most enthusiastic security team, operating alongside the most advanced technology, will not succeed without access to clearly defined, and easy to understand, operating procedures.

Principle No 7: It is essential that every organisation carries out regular tests and drills of its security systems. A security system that has never been tested and drilled is an unknown quantity and may fail to operate as it should in the case of a real situation. Penetration tests are another useful tool in terms of highlighting security strengths and weaknesses.

Principle No 8: The final principle concerns the need to carry out internal and external security audits. The value of audits cannot be overstated and they will help determine whether the current policy and strategy is still adequate enough to contain all the established risks and threats. It should be remembered that threat levels and circumstances all change over time, so a system must be constantly kept under review.

2. Definition of Iconic Sites

Iconic sites have been described as *'a site that is important or impressive because it seems to be a symbol of something'*. An example of an iconic site would be the Tower of London or the Eiffel Tower, as they are symbols of the cities and countries in which they are located. It is not uncommon, however, for purely commercial sites to also be described as iconic, e.g. The Gherkin (Swiss Re building in the City of London). By their very nature, iconic sites and

premises will be considered high risk from a security aspect, as historically terrorist and direct action/protest groups will target such installations, e.g. the World Trade Centre in New York ('Twin Towers') on 9/11, and the London Underground system on 7/7. Over the past few years, Islamic terrorists have targeted iconic places of entertainment, such as the Bataclan theatre in Paris, and the Manchester Arena.

As a consequence, a site that may appear not to be iconic in strict terms, may be perceived as such by others.

Additionally, premises which are adjacent to, or in close proximity to iconic sites are, by their very location, vulnerable to the collateral threats and damage that may be caused to such sites in the event of a terror or other attack.

3. Sources of Threats

There essentially, five key categories of threat that could potentially affect Iconic and high-risk sites:

- Threat from Global and Regional Terrorism
- Organised Crime
- Opportunist Criminality (e.g. random theft, acts of violence, and sexual crime)
- Extreme single-issue or political activists
- Vandalism and Anti-social Behaviour

4. Terror Threats/Threat Level

Global Terror Threats

The United Kingdom remains under threat from further terrorist attacks along the lines of those that have occurred in London on 7 July 2005, Glasgow 2008, Woolwich 2013, the terrorist attacks in France, Germany, Belgium, and elsewhere. This has proved to be the case following last year's fatal attacks on: Westminster Bridge; the Palace of Westminster; Manchester Arena; London Bridge/ Borough Market; the Finsbury Park Mosque; the attempted

atrocity at Parsons Green Tube, and the ram attack by a vehicle hitting the barriers protecting the Houses of Parliament. These terrorist attacks have been the most sustained and deadly since the 7/7 suicide bombings. Such attacks are likely to be to be perpetrated or inspired by fanatical groups directed by or linked to Daesh (Islamic State), or Al Qaeda, or in the case of the attack on the Finsbury Park Mosque, perpetrated by anti-Moslem extremists.

These attacks indicate that the threat is ongoing and increasing in intensity. Andrew Parker, Director General of MI5, stated in October 2017 that the UK had seen a dramatic uplift in the threat from Islamist terrorism. A report published recently indicates that 2017 was the most intensive year, in terms of contemporary terrorist threats, the scale of anti-terrorist operations and interventions. The report confirms that a large number of potential terrorist activities and attacks were thwarted by the security services working in tandem with the specialist anti-terrorist commands of the 44 constabularies (including British Transport Police) operating throughout the UK, and which resulted in more than 400 arrests for terrorism offences in 2017.

Northern Ireland Related Terrorist Threats

Turning now to the threat emanating from Northern Ireland, the establishment of power sharing in Northern Ireland has led to a cessation of wide-scale hostilities both there and also on the UK mainland, although attacks by dissident IRA groups in Northern Ireland have continued. There is thus a potential threat from dissident IRA groups, such as Real IRA, Continuity Movement, and Oglaigh na Eireann.

Whilst the targets of these dissident groups have generally focussed on members of the Police Service of Northern Ireland, there is a risk that such groups could once again target key British institutions on the mainland.

The current threat level from international terrorism for the UK is now assessed as: **SEVERE**
The threat level for Irish related terrorism is set separately for Northern Ireland and Great Britain. The threat from Northern Ireland-related terrorism in Great Britain is set at **MODERATE** In Northern Ireland it is: **SEVERE**
NOTE: • **CRITICAL** means that a terrorist attack is imminent • **SEVERE** means that a terrorist attack is highly likely • **SUBSTANTIAL** that an attack is a strong possibility • **MODERATE** that an attack is possible but unlikely

It is not uncommon for extremist terror groups to target 'secondary' or 'soft' targets in order to make their point, or to grab media headlines. The atrocities perpetrated against the Bataclan Theatre in Paris, and Manchester Arena, are both classic examples of the vulnerability of soft/iconic targets.

The threat of international terrorism emanates from a diverse range of sources, including Daesh (the so-called 'Islamic State' (IS)), Al Qaeda and associated networks, and those who share Al Qaeda's ideology but do not have direct contact with them. A threat could manifest itself from a lone individual or group, rather than a larger network.

Extreme right-wing Threats

The growing threat of far-right terrorism has been highlighted in recent months, by both the Counter-Terrorist Police, and the Security Service (MI5).

Former Assistant Commissioner Mark Rowley, of the Met Police confirmed that four extreme-right terror plots were disrupted during 2017. Mr Rowley also warned that far-right extremists are working in similar ways to Islamist extremists.

He said they create intolerance, exploit grievances, and generate distrust of state institutions. One of the four alleged far-right plots disrupted was that of white supremacist Ethan Stables. Earlier this year, Stables was convicted of plotting an axe and machete attack on a gay pride event at a pub in Barrow.

Mr Rowley also stated that Islamist and right-wing extremism is reaching into our communities through sophisticated propaganda and subversive strategies creating and exploiting vulnerabilities that can ultimately lead to acts of violence and terrorism.

Referring to the banned group National Action, Mr Rowley confirmed that for the first time the UK has a home-grown proscribed white supremacist, neo-Nazi terror group, which seeks to plan attacks and build international networks. In 2017 the security service MI5 joined the fight against the right-wing terrorist threat. There are currently more than 600 live investigations and more than 3,000 people of interest at any one time.

5. Methodology & Modus Operandi of Terror Groups & Individuals

The nature of terrorist threats can take a number of forms, as terrorists may use a variety of methods of attack to achieve their objectives. These may include explosive devices (IEDs and VBIEDs), suicide bombings, firearms, cold weapons, such as knives, missiles, vehicle ramming attacks, kidnapping, infiltration, and cyber-attacks.

There is continued concern within the policing, security and intelligence services community that Daesh and/or Al Qaeda linked terrorists may seek to carry out Mumbai/Bataclan style combined shooting/bombing attacks (now commonly referred to as “Marauding” or “Swarm” attacks) in the UK. We have witnessed such attacks in Paris directed against an iconic theatre, football stadium and restaurants and bars.

6. Addressing & Coping with Terror Threats

As mentioned above, it is the responsibility of the managers and operators of iconic and high risk sites to procure professional security risk and threat assessments. Of course, it is important to note that terrorists and other adversaries, such as direct action and protest groups, will frequently conduct hostile reconnaissance on their target sites prior to launching an attack or other hostile action. The ability of security personnel and indeed employees of organisations at risk, to identify and report hostile reconnaissance is of vital importance. Organisations at risk are reminded to take all appropriate measures to educate and inform their employees and security teams of the need to remain vigilant in the face of hostile reconnaissance and information gathering by adversaries of whatever ilk.

Security Patrols

Security patrol members who engage in external patrols should pay particular attention to the following potential indicators of hostile intent:

- Suspicious vehicles parked in restricted areas; or being driven erratically; or with occupants taking photographs or video footage from those vehicles
- Persons acting suspiciously who may be taking photographs or video footage; or who are asking intrusive questions about premises ownership, usage or security

Security teams can also be equipped with two-way radios, as well as mobile phones, body worn video (BWV), notebooks, high-visibility clothing and, where necessary, torches.

Security personnel should also be reminded never to place themselves in personal danger, where they perceive a serious physical threat. They must be reminded to report any suspicious activity without hesitation to their Security Controller or other relevant Manager.

Businesses should develop a 'security culture', with buy-in from all levels of the business including the very top (often the most difficult to persuade). Staff should be trained to understand what is expected of them in an emergency

7. Guidance for Customers and their Security Personnel

PLEASE NOTE: The Guidance in this section (7) is taken from NaCTSO Guidance Document 1/2015 (National Counter Terrorism Security Office)

Developing Dynamic Lockdown Procedures

This note provides guidance to develop procedures to dynamically lockdown their sites in response to a fast moving incident such as a firearms or weapons attack, either directly at the site or in the vicinity. Due to the differences between the vast array of sites in the UK it is not possible to give prescriptive advice, however this guidance details planning considerations applicable to most sites.

What is dynamic lockdown?

Dynamic lockdown is the ability to quickly restrict access and egress to a site or building (or part of) through physical measures in response to a threat, either external or internal. The aim of lockdown is to prevent people moving into danger areas and preventing or frustrating the attackers accessing a site (or part of). It is recognised that due to their nature some sites may not be able to physically achieve lockdown.

Why develop dynamic lockdown?

Those seeking to conduct attacks often undertake a level of planning including hostile reconnaissance. All opportunities to detect and deter threats at the attack planning phase should be taken. Presenting a strong security posture through visible and effective activity, for example by staff awareness and reporting processes, efficient use of CCTV, deterrent communications and active security zones.

In preventing an attack has not been possible, the ability to frustrate and delay the attacker(s) during the course of the attack and reduce the number of potential casualties can be greatly increased through dynamic lockdown. Advance planning of what needs to be done to lockdown a site and recognising the need for flexibility in those plans will save lives.

Planning should consider;

- How to achieve effective full or partial lockdown
- How to let people know what's happening
- Training your staff
- STAY SAFE principles:

"Stay Safe" is a short film capturing the actions that people should take in the event of a firearms or weapons attack. It contains the main messages of '*Run, Hide and Tell*', details of which can be found further on in this document.

How to achieve dynamic lockdown

- In your planning you should identify all access and egress points in both public and private areas of the site. Remember, access points may be more than just doors and gates.
- Identify how to quickly and physically secure access/egress points Identify how your site can be sectored to allow specific areas to be locked down
- Staff roles and responsibilities should be included in the plans.
- Staff must be trained to act effectively and made aware of their responsibilities
- Stopping people leaving or entering the site – direct people away from danger
- Ability to disable lifts without returning them to the ground floor should be considered
- Processes need to be flexible enough to cope with and compliment invacuation and evacuation

How to let people know what's happening

Various options exist depending on the nature and occupancy of the site, these include;

- Public Address (PA) system
- Existing internal messaging systems; text, email, staff phones etc.
- "Pop up" on employees computers / internal messaging systems Dedicated "Lockdown" alarm tone
- Word of mouth

For multi occupancy sites, methods of communication between all businesses need to be considered. Likewise, working with surrounding businesses will not only benefit situational awareness but build effective lines of communication.

Note: Use of fire alarms should be avoided to reduce incorrect response to an incident.

Training your staff

Due to the fast moving nature of incidents that require lockdown it is important that all staff are able to act quickly and effectively.

- Train all staff using principles of "Stay Safe"
- Ensure people know what is expected of them, their roles and responsibilities
- Check staff understanding
- Regularly test and exercise plans with staff
- Regularly refresh training

Firearms and weapons attack

'Stay Safe' principles (Run Hide Tell) give some simple actions to consider at an incident and the information that armed officers may need in the event of a firearms and weapons attack**.**

Run

- Escape if you can.
- Consider the safest options.

- Is there a safe route? RUN if not HIDE.
- Can you get there without exposing yourself to greater danger?
- Insist others leave with you
- Leave belongings behind.

Hide

- If you can't RUN, HIDE.
- Find cover from gunfire.
- If you can see the attacker, they may be able to see you.
- Cover from view does not mean you are safe, bullets go through glass, brick, wood and metal.
- Find cover from gunfire e.g. substantial brickwork / heavy reinforced walls.
- Be aware of your exits.
- Try not to get trapped.
- Be quiet, silence your phone.
- Lock / barricade yourself in.
- Move away from the door.

Tell

Call 999 - What do the police need to know?

- Location - Where are the suspects?
- Direction - Where did you last see the suspects?
- Descriptions – Describe the attacker, numbers, features, clothing, weapons etc.
- Further information – Casualties, type of injury, building information, entrances, exits, hostages etc.
- Stop other people entering the building if it is safe to do so.

Armed Police Response

- Follow officers' instructions.
- Remain calm.
- Can you move to a safer area?
- Avoid sudden movements that may be considered a threat.

- Keep your hands in view.

Officers may

- Point guns at you.
- Treat you firmly.
- Question you.
- Be unable to distinguish you from the attacker.
- Officers will evacuate you when it is safe to do so.

You must STAY SAFE

- What are your plans if there were an incident?
- What are the local plans? e.g. personal emergency evacuation plan.

8. Coping and Responding to Emergencies and Serious Incidents

Managing and responding to emergencies and other serious incidents, such as terror attacks, should be set out in the organisation's Security Procedures. Where contract guarding teams are in place, their own actions and responsibilities will be set out in their Assignment Instructions. It is important to ensure that the various roles and responsibilities and detailed responses contained in those documents are harmonised so that there are no discrepancies in the detailed actions being implemented. An example of where discrepancies or contradictions may occur, is where the organisation's procedures for evacuation assembly points may be at variance with those set out in the guarding contractor's Assignment Instructions.

'Evacuation or Invacuation'

One of the most consistent attack methodologies is the use of multiple and co-ordinated attacks to cause mass casualties. This in itself brings into focus what we should do in the event of a terrorist attack on premises. Automatic evacuation could mean taking those who are in the relative safety of a building out into a highly dangerous environment of secondary fragmentation and falling glass and of course possibly into another explosion.

Of course great care must be employed when deciding whether to advise invacuation as the automatic response, especially if the building is on fire or in danger of collapse.

What is Invacuation?

Invacuation is the opposite of evacuation, i.e. refuge is sought within the building following an attack, as opposed to evacuating the building to the relevant assembly point. If invacuation is necessary, this should be carried out according to directions of the responsible manager or decision making team.

Actions to be considered during an attack include:

• Taking immediate cover away from windows and doors, which should remain closed

• Staff and visitors should only leave when directed to do so by the Emergency Services. Clear instructions and procedures must be put in place to ensure all staff/visitors are aware of the need to stay indoors, and where the safest place would be

• Safe places can often be found towards the centre of the building away from glass or external doors, but you should always seek advice from a structural engineer to identify protected spaces within your building

Practical Considerations for Evacuation and Invacuation

• Consideration should be given to access to water and toilet facilities if sheltering for extended periods of time

• You should agree your evacuation/invacuation plans with the Police and other Emergency services, and your trusted neighbours

• Ensure that all staff are aware of the plans and that appropriate measure are in place to assist any disabled colleagues

• Terrorists will sometimes use an attack method where they set off one explosion in order to get potential victims to evacuate themselves to a more open environment, where they can be easier to attack either with a secondary device, and/or firearms

• The increased use of firearms in terrorist attacks ('Swarm Attack'), also brings into question our usual response to an emergency
• The natural reaction to evacuate from a building could potentially increase the death toll, as well as increase the fear value associated with the attack
• In Bali, for example, a small device was exploded inside a nightclub to move victims outside into the path of a large car bomb (VBIED) causing catastrophic loss of life

Sharding Glass

We also know that in urban environments (such as the Manchester bombing in 1996) flying (sharding) glass has often caused the majority of injuries in a bomb blast, hence the evolution of 'invacuation' as a contingency.

Useful Equipment for Contingencies and Emergencies

'Grab Bags' and Emergency Equipment

- List of Contacts (laminated) staff, head office, etc.
- Emergency Plans and Floor plans
- Incident Log (consider dictaphone), notebook, pens, markers, etc.
- First aid kit (designed for major emergencies) consider large bandages, burn shields or cling film, large sterile strips, cold packs, baby wipes as well as standard equipment
- Torches and spare batteries (or wind up)
- Glow sticks
- Radios for monitoring media (plus spare batteries)
- Two-way Radios (fully charged plus spare batteries)
- High visibility jackets
- Loud hailer and spare batteries
- Hazard and cordon tape
- Plastic macs/foil blankets/bin liners
- Dust/toxic fume masks
- Water (plastic container) and chocolate/glucose tablets
- Computer back-up tapes/disks/USB memory sticks or flash drives

Consideration to be given in the case of premises fire and/or collapse

In circumstances where evacuation is the obvious answer, those in key areas within businesses must be aware of the potential consequences of each option so that they can make an informed decision. Businesses should also understand that they will be responsible for their staff and customers (if a terrorist attack takes place), and have appropriate evacuation and invacuation plans.

In line with Corps Consult's Eight Principles of Security, such plans and procedures should be regularly tested to ensure their integrity.

9. Security Alerts and Intelligence Sharing

It is prudent to monitor the various alert systems and services provided electronically by agencies such as the Police, CSSC and the Griffin network. Participating in local security forums (which enable local threats and intelligence to be shared in a collaborative manner by trusted organisations with common interests) is also a useful way to glean local information and intelligence.

10. Business Continuity

To help mitigate against any incident which may potentially impact upon normal modes of operation (be it terrorist related or otherwise), a Business Continuity Plan (BCP) needs to be put in place, which should be designed to:

- Help protect employees
- Minimise business impact
- Help protect customer interests

Each individual threat-scenario identified within the BCP, must be evaluated via a formal Risk Assessment, with the significance of each threat and its potential impact upon businesses, being determined via a Business Impact Assessment (BIA). The recommended actions for ensuring business continuity and a speedy return to a normal mode of operation, should then be listed within a threat-specific Action Plan.

11. Further Advice/Guidance

Please feel free to contact Corps Consult as follows:

Email: mbluestone@corpssecurity.co.uk

T: 0207566 0516