Advice for security managers of crowded places following a change of threat level to CRITICAL

1. Introduction

The aim of this advice is to provide advice to security managers of crowded places following a change of the threat level to CRITICAL. There are a number of operational and tactical options you may wish to consider.

Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities.

Information about the national threat level is available on the MI5 – Security Service website.

2. Threat Level Definitions

There are five levels of threat which are defined below:

CRITICAL	An attack is expected imminently
SEVERE	An attack is highly likely
SUBSTANTIAL	An attack is a strong possibility
MODERATE	An attack is possible but not likely
LOW	An attack is unlikely

There is no specific intelligence, the assessment is generic and does not identify any sector or detail of locations or timings. As a consequence of the change in threat level it is recommended that those responsible for security review their plans and operations. You may wish to consider some of the options listed below.

3. Response Levels

The UK Government Response Levels provide a general indication of the protective security measures that should be applied at any particular time. They are informed by the threat level, but also take into account specific assessments of vulnerability and risk. During any incident leadership is key, make a dynamic risk assessment and take responsibility. Decisive individuals will save lives.

There are three levels of response **EXCEPTIONAL**, **HEIGHTENED** and **NORMAL**.

Response levels equate to threat levels and tend to relate to sites, whereas threat levels usually relate to broad areas of activity. There are a variety of site specific security measures that can be applied within each response level, although the same measures will not be found at every location. The security measures deployed at different response levels should not be made public, to avoid informing terrorists about what we know and what we are doing about it.

To support your planning the threat level and response levels are combined in the table below.

Threat level and definition	Response level	Description
Critical An attack is expected imminently	Exceptional	Maximum protective security. Critical measures to meet specific threats and to minimise vulnerability and risk
Severe An attack is highly likely	Heightened	Additional and sustainable Substantial and Severe protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk
Substantial An attack is a strong possibility		
Moderate An attack is possible but not likely	Normal	Routine protective security. Low and Moderate measures appropriate to the business concerned
Low An attack is unlikely		

4. Additional Information

There are some simple, practical actions you can take immediately to help improve the security of your venue:

Risk Assessment

- Carry out a risk assessment that is specific to your venue

Building Response Level

- Regularly review the response level for your site or venue at security meetings
- Clearly display signage informing staff of the building response level. This should not be displayed in public areas

Security officers posture and activity

- **Proactive engagement and staff briefings.** One of the most disruptive measures to counter terrorists and wider criminality is a security force that appears to be vigilant and proactively engages with the public. Terrorists and criminals do not want to be spoken to by any member of staff and will actively avoid engagement – this should be polite but professional. If they are spoken to it is likely to make them feel very uncomfortable and exposed. **Staff briefings** will enable your security officers to understand the importance of proactive engagement and they should be encouraged to do this where practical and reasonable to do so. For example, if security officers patrol to areas in a car (such as a car park), encourage them to get out of the car and engage with people, as simple as saying good morning.
- **Unpredictable security measures.** Unpredictability results in uncertainty and erosion of confidence in the mind of the hostile who need this predictable security arrangements so that they can plan for likely success. Where practical and reasonable build in unpredictability for example, timings and types of assets and search regimes deployed at your site.

- **'Recruit' staff to be vigilant for and immediately report suspicious activity and items.** Use existing staff communications such as shift briefings, intranet etc. to inform as to what suspicious activity may look like, to trust their instincts and report immediately to the security control room/police. In these communications convey how their reports will be taken seriously and investigated and where possible showcase where previous staff reporting has led to outcomes, both where there have been benign and security outcomes; this helps promote confidence in reporting.

The counter measures to be implemented at each response level are a matter for individual premises or organisations and will differ according to a range of circumstances. All protective security measures should be identified in advance of any change in threat and response levels and should be clearly notified to those staff who are responsible for ensuring compliance. It is important to train staff and the conduct rehearsal exercises for each response level. The table below provides a number of protective security options you may wish to consider to consider.

For further information visit:
www.nactso.gov.uk, www.cpni.gov.uk, Cabinet Office, Emergencies: preparation, response and recovery, Emergency Planning.

Security Checklist

INITIAL ACTIONS

1. Review your security plans
2. Identify your risks, based on the current threat
3. Review your Business Continuity Plans
4. Decide what you need to protect, identifying critical operations and functions
5. Increase staff vigilance – through briefing
6. Review Evacuation, Invacuation and Lockdown procedures. Ensure you have plans for vulnerable staff and visitors. Have you designated marshals to support this activity.
7. Identify 'protected spaces'
8. Review your Emergency Assembly Point

PREPAREDNESS

1. Ensure First Aid Kits are fully stocked and staff know where they are kept
2. Ensure Crisis Incident Kits (grab bags) are available and up to date

COMMUNICATION

1. Brief staff – ensure they understand their roles and responsibilities
2. Engage with neighbours, partners and suppliers
3. Ensure you are able to alert staff and visitors of any imminent or immediate threat or incident
4. Provide prior notification to staff and visitors of enhanced security measures, encouraging them to arrive in plenty of time and encourage them to bring minimal possessions
5. Monitor news and media channels
6. Develop pre-scripted messaging and alerts and determine how these will be communicated to staff and visitors

PERSONNEL

1. Maintain an up to date list of personnel (Do HR update leavers and joiners?)
2. Consider extending staff shifts where appropriate
3. Consider cancelling leave where appropriate
4. Consider cancelling non-urgent business or visitors where appropriate to your venue
5. Identify if you have sufficient staff for critical roles such as your control room
6. Review requirements for Personal Protective Equipment (PPE) for security staff

TRAINING

1. Ensure staff understand how to respond to a terrorist incident. see ETHANE
2. Are staff first aid trained
3. Review and deliver training to your staff and conduct rehearsal exercises

STAFF VIGILANCE

1. Do **ALL** staff understand how to respond effectively to reports of suspicious activity, behaviour and items when reported by the public. Who they should report to internally and when to report to police using 999
2. Disrupting hostile reconnaissance: Ensure staff understand how to identify suspicious behaviour (Do you have a challenge culture? – see CPNI website)

3. Suspicious Items: Ensure staff understand how to respond to suspicious items. Do staff know the HOT principles?
4. Ensure all staff and visitors wear passes
5. Where entry is restricted, check the visitors identification prior to allowing access to the site

PHYSICAL SECURITY

1. Enhance your security presence where appropriate, consider staff patrolling in high visibility clothing
2. Ensure CCTV is working effectively and monitored
3. Review your access controls. Where appropriate close unnecessary entrances to prevent unauthorised access
4. Ensure infrastructure, such as signage, lighting, floor level signs, stairs etc. are clearly marked and labelled.
5. Prepare floor plans
6. Establish if your control room is capable of being operationally effective against different attack types and can be secured and protected
7. Check critical systems and equipment such as PA systems
8. Ensure control rooms have alternative means of communication such as mobile phones with spare batteries, chargers etc.
9. Consider the protection requirements for any queues of people created by additional search measures (CCTV, position of the queue etc.)

SEARCH AND SCREENING

1. Business as usual search and screening (looking for prohibited items) should, when done well, provide a very good capability to detect larger threat items concealed about the person
2. You will have a finite amount of security and screening resources, focus on addressing your highest priority threats
3. Be clear about what the search process is aiming to detect, who you need to screen and where you will conduct the process
4. Define lists of prohibited items. Communicate this both to customers and personnel conducting the search
5. Prior notification (at point of sale or media) of these extra security measures and encouraging people to arrive early, will smooth peaks and allow safe and effective searching
6. Provide effective public address messaging to people as they approach, asking people to prepare for additional search and screening. This should reduce unacceptable delay

7. Consider initial search and screening on the approach or outside the venue, for example a visual check inside jackets and bags
8. Conduct search and screening measures efficiently, effectively and politely. Aim to maximise screening throughput (to minimise queues that may be targeted)
9. **Bags and other items** should be searched to the extent required to provide confidence that no items of concern are present. Manual bag searches should be, proportionate, systematic, consistent and safe for the person conducting the search. Always look where you are searching
10. **Manual person searches** should be considered to the extent required to provide confidence that no larger threat items are present. Engage the customer and obtain their permission. Consider whether search should be a condition of entry if it is not already. Search systematically from head to toe. Pay particular attention to bulky and baggy clothing. Continue the search to the end, even if something is found. Do not be intimidated or distracted. Use hands in a firm sliding motion. Screeners should always be the same sex as the customer. Where appropriate ask the customer to remove pocket items. Consider the privacy needs of the individual
11. Ensure your site or venue is searched on a regular basis but not at predictable times or in a predictable way
12. Ensure you maintain your search regime for the lifecycle of the event including prior to the commencement, during and post event
13. Determine whether you allow vehicles into your venue and if you intend to search vehicles entering your venue
14. Train search staff to search safely and effectively
15. Ensure all staff are aware of the response when they locate threat items
16. There a number of other tactical options available for search and screening , specialist advice should be sought from the CPNI website or your local Counter Terrorism Security Advisor.

SECURITY PERSONNEL

Depending upon their responsibilities an effective security guard must be able to demonstrate they can respond effectively to a number of scenarios including:

1. Do you security staff understand how to respond effectively to reports of suspicious activity, behaviour and items when reported by the public. Who they should report to internally and when to report to police using 999, 101 or call the Anti-Terrorist Hotline 0800 789 321
2. Initial actions at a terrorist incident, see ETHANE
3. Ensure you maintain your search and patrol regime for the lifecycle of the event including prior to the commencement, during and post event. Consider a patrol sweep of the public areas before, during and after an event looking for suspicious items and behaviours. Patrol

areas might include areas close to the site, pick up zones and transport hubs. Ensure those staff can communicate effectively with a control room.

4. The different terrorist threat levels, building response levels, and different activities required should there be an increase in threat
5. Hostile reconnaissance, how to patrol effectively to disrupt activity, identify and respond to suspicious behaviour
6. Suspect items, the 'four Cs' protocols and the HOT principles
7. Chemical, biological and radiological incidents, how to recognise and respond using STEPS 123
8. A firearms and weapons attacks and the Run, Hide, Tell principles
9. Evacuation, invacuation and lockdown procedure demonstrating knowledge of the emergency assembly points
10. How to search a site effectively
11. The basic principles of good housekeeping and how it reduces the opportunities for an attack
12. How to respond appropriately to a bomb threat
13. Using emergency equipment such as defibrillators etc.
14. Use of incident logs and checklists that facilitate an effective response to incidents such as terrorist incidents, bomb threats etc.

GOOD HOUSEKEEPING

1. Where your risk assessment determines it is necessary, examine opportunities to reducing reasons for crowds to dwell such as reducing or removing or relocating activities that are attractive, such as street entertainers, mobile food outlets etc. Consider increasing patrols in these areas. Consider carefully where these activities take place.
2. Have you reviewed the use and location of all waste receptacles in and around your venue or event, taking into consideration their size, proximity to glazing and building support structures? Consider repositioning to areas that are not crowded
3. Are the bins emptied regularly?
4. Are external areas, entrances, exits, stairs, reception areas and toilets kept clean, tidy and well lit? Where possible reduce areas where items can be concealed
5. Do you keep furniture to a minimum to provide little opportunity to hide devices, including under chairs and sofas?
6. Do you use seals/locks to secure maintenance hatches, compacters and industrial waste bins when not required for immediate use?
7. Consider arranging vehicle deliveries for times where the fewest number of people are on site. Consider adopting time windows where no deliveries will be accepted.

8. Do you screen all your mail and can you isolate your mail processing area?
9. Have you tested and exercised for a terrorist incident in the last 12 months? Do staff understand their roles and responsibilities?
10. Are relevant staff and deputies trained and competent in managing bomb threats?
11. Do you regularly check the content of first aid kits, crisis management packs and firefighting equipment?
12. Have you checked your CCTV to ensure it is working effectively and has sufficient coverage inside and outside?
13. Have you taken into account the location of street vendors (e.g. flower sellers, newsstands and refreshment stalls) so as not to impact upon evacuation routes, assembly points, exits or entrances?
14. Are cycle racks and lockers positioned away from crowded areas? Is CCTV monitoring necessary?