Lincolnshire Event Safety Partnership

safe events across the county

COUNTER TERROR GUIDANCE FOR EVENT ORGANISERS

Version 3
February 2022

CONTENTS

AIM OF THIS DOCUMENT

The aim of this document is to provide advice to event organisers on a range of counter terrorism considerations that they may wish to include in their event management plans.

INTRODUCTION

Terrorist attacks in the UK are a real and serious danger. Terrorists continue to target crowded places largely because they are usually locations with limited protective security measures and therefore afford the potential for mass fatalities and casualties. Terrorism also includes threats or hoaxes designed to frighten and intimidate.

The threat continues to be driven by inspired self-initiated terrorists or small cells looking to conduct low-complexity attacks using low-sophistication methodologies. The Centre for the Protection of National Infrastructure (CPNI) assess that future attacks are most likely to be blunt or bladed weapon attacks or vehicle as a weapon attacks. Attacks using homemade explosives to produce improvised explosive devices or firearms cannot be ruled out.

GOOD HOUSEKEEPING

Good housekeeping improves the ambience of your premises, reduces the opportunity for placing suspicious items or bags and helps you manage false alarms and hoaxes. Items left insecure on site, such as flammable liquids, tools, scaffolding poles and ladders, could be used by terrorists and criminals. It's therefore important that they are safely secured whenever they

You can reduce the number of places where devices may be left by considering the following points:

- Avoid the use of litter bins in vulnerable areas (e.g. near crowded locations, glazing and support structures). Monitor vulnerable areas with CCTV and make sure there are regular cleaning regimes in place.
- Review the management of all your litter bins and consider the size of their openings, their blast mitigation capabilities and location.
- The use of clear bags for waste disposal makes it easier to conduct an initial examination for any suspicious items.
- Review the use, placement and security of any compactors, recycling sorting points, wheelie bins, skips and metal bins used to store rubbish within service areas, goods entrances and near areas where crowds congregate.
- Your operations manager should have an agreed procedure in place for the management of contractors, their vehicles and waste collection services. The registration mark of each vehicle and details of its occupants should be known to the security staff or manager in advance of their arrival.
- Keep public, communal and external areas (such as exits, entrances, lavatories, service corridors and yards) clean, tidy and well lit.
- Keep the fixtures, fittings and furniture in such areas to a minimum, ensuring there is little opportunity to hide devices.
- Lock and check unoccupied offices, rooms and store cupboards.
- Place tamper-proof plastic seals on maintenance hatches.
- Ensure that all staff are trained in bomb threat handling procedures, or at least have ready access to instructions, and know where these are kept.
- Review your CCTV system to ensure that it is working correctly and has sufficient coverage both internally and externally.
- Ensure first-aid kits and fire extinguishers are checked regularly and ensure that they have not been interfered with. Any used items should be replaced. Are a sufficient number of staff trained in first aid for a terrorist type attack?
- Security managers should consider a secondary secure location for use as a control room as part of their contingency planning.
- Ensure street vendors, cycle racks, lockers and bins do not impede evacuation routes, assembly areas, exits or entrances.
- Ensure cycle racks and lockers are placed away from crowded areas. Monitor with CCTV if necessary.

HOSTILE RECONNAISSANCE

Hostile reconnaissance is the term given to the gathering of information from people, places and websites to inform the planning of a hostile act against a specific target.

Objectives of Hostile Reconnaissance:

- Identify a target
- Discover weak spots (vulnerabilities)
- Assess the level and type of security
- Consider the best method of attack
- Inform the best time to conduct the attack
- Assess the likelihood of success

Security of the event should be focussed in the following manner: to **deny** the hostile the opportunity to gain information, to **detect** them when they are conducting their reconnaissance and to **deter** them by promoting failure through messaging and physical demonstration of the effective security.

Deny

Denying the hostile the information they need to fulfil their information requirements is the first step an organisation can take in forcing the hostile to either disregard its site as a target, or by ensuring that they have to undertake further, potentially detectable, reconnaissance, e.g. removing or modifying information from public-facing websites and educating employees on what kind of information hostiles will be looking to use (from their social media accounts, for example).

Denying the hostile the information they need can also mean creating uncertainty and unpredictability about security arrangements at a site. For example, unpredictable timing, type and location of security patrols make it difficult to assess a pattern of activity that they can exploit with any confidence.

Sites / event managers are encouraged to AUDIT information available online; ADAPT it where there is information which could be useful to a hostile; AMPLIFY protective security measures and mitigations in place.

Detect

Hostiles know they are on site for malicious reasons and that their behaviour might appear out of the norm. This makes them more anxious or paranoid and therefore, potentially susceptible to detection. This natural anxiety can be amplified by communicating and demonstrating an effective range of detection capabilities at the site. Vigilant and engaged security officers with timely and appropriate interventions can be particularly powerful in addition to well-sited CCTV and control rooms with proactive operators looking for suspicious activity.

Owing to hostiles anxiety they will not want to be spoken to by security. Saying hello in a friendly manner may serve the dual purpose of extending good customer service whilst deterring them.

Deter

Deterrence is a vital component of disrupting hostile reconnaissance.

Press media and social media will be used to reassure the public that security is a prime concern of the organisers and all members of staff should be aware that questions relating to possible attacks are likely in all contact/interviews with the media. All promotion of security capability MUST be truthful. If it isn't then, if the deceit is uncovered, all security claims may be discredited.

Identifying Suspicious Behaviour

Remember to focus on behaviour not appearance. You must understand what is normal and 'every day'. Take time to understand your working environment. Learn to spot the difference between normal and unusual/suspicious behaviour. Be alert to the threat.

On foot

- Loitering in restricted or non-public areas
- Is that person really taking a selfie or a photograph of something else?
- Paying significant interest to: entrances, exits, CCTV or security staff, taking photos
- Concealing face / identity
- Using disguises (PPE, official looking fluorescent clothing or lanyards for example)
- Asking unusual or security related questions
- Avoiding security staff
- Activity inconsistent with the nature of the building or area

From a vehicle

- Vehicles parked out of place
- Vehicles retracing the same route
- Trust your instincts, if you see anything suspicious take action

Challenging and Reporting of Suspicious behaviour

After conducting a dynamic risk assessment: You SHOULD approach a person that has been acting in a suspicious manner and politely ask them to account for their actions.

- Always remember - Stopping a hostile before they can carry out their plans will ultimately save lives
- You cannot spot a hostile from their appearance, age, ethnicity, gender or clothing
- You can identify and report their suspicious behaviour.

What information do the police need from you?

If you become aware of suspicious activity, you should dial 999 if the person is still on scene and you need an immediate police response.

Providing the following detail is useful:

- When did this happen? An accurate date and time of the incident
- Where did this happen? The venue, address and specific details about the location

- Who did you see? A detailed description of the person and what they were wearing and/or vehicle and direction of travel. The name, date of birth, address, and any phone numbers obtained of the person if they were stopped.
- Why you thought it was suspicious?
- What actions you took at the time?

Remember: it is always better that police are called while the person or vehicle is still at the scene. If the person has left the scene and their route taken is unknown, or a significant period of time has elapsed since the incident, i.e. several hours, then contact the Anti-terrorist hotline on 0800 789321

Hostile Reconnaissance Checklist

When an organisation is clear on the nature of the threats it faces and has understood the Deny, Detect, Deter principles, then vulnerability to online and physical hostile reconnaissance can be reduced by considering the following six themes:

- Having a secure online presence
- Operating a robust entry process
- The hostile reconnaissance threat is understood
- There is a strong staff security awareness
- The site operates vigilant and professional security
- There is a deterrence strategy

See Check and Notify – ScaN

See, Check and Notify (SCaN) aims to help businesses and organisations maximise safety and security using their existing resources. Your people are your biggest advantage in preventing and tackling a range of threats, including terrorism, criminal activity and protest. SCaN helps ensure that individuals or groups seeking to cause your organisation disruption and / or harm are unable to get the information they need to plan their actions. It also empowers your staff to know what suspicious behaviour to look for, and what to do when they encounter it. Additionally, the skills they learn will help them to provide an enhanced customer experience.

Further information on SCaN

Security Staff Powers

If part of the suspicious behaviour involves the taking of photographs, understand your powers:

- There is NO power in law to prevent a person from taking a photograph of anything or any person in a public place
- There is NO legal power to require or ask that any images taken are to be deleted
- Security personnel have NO legal power to ask to view images taken
- Security personnel have NO legal power to seize any camera or phone used to take any image
- If police are called, a person CANNOT be detained by security staff awaiting the arrival of police
- Powers to search and seize are ONLY available to a Police Officer

A suspicious behaviours reporting form is at Appendix A

BOMB THREATS AND IMPROVISED EXPLOSIVE DEVICES

Bomb Threat

Most bomb threats are usually made over the phone. The overwhelming majority are hoaxes, often the work of malicious pranksters, although terrorists also make hoax calls. However, until shown to be otherwise, all bomb threats should be treated as if they are genuine and the correct procedures followed.

Genuine threats are rare however a hoax call is a crime and, no matter how ridiculous or unconvincing should be reported to the police.

Calls from terrorists and extremists fall into two kinds:

1. Bomb threats when none has actually been planted. These hoaxes may not be merely malicious but designed to disrupt, to test reactions or to divert attention;
2. Bomb threats warning of a genuine device. These may be attempts to avoid casualties, but they also enable the terrorist to blame others if there are casualties.

Even genuine threats are frequently inaccurate with regard to where and when a bomb might explode. Staff receiving a bomb threat may not always be those trained and prepared for it, namely temporary reception or office personnel, however, the member of staff receiving such a call should attempt to assess a threat's accuracy, truth or origin and form their own impression of the caller. The member of staff receiving a call may be temporarily in a state of shock at the threat, which will be the closest that many people ever come to acts of terrorism. Despite this the member of staff should attempt to pass on a threat promptly, in as much detail as possible, to those tasked with deciding what action to take. Staff should always remember to distinguish between calls referring to their own building and those warning of a bomb elsewhere.

Office and reception staff should understand their important role in recording and communicating any bomb threat.

Receipt of a call

Such threats or hoaxes will probably be made over the telephone the following guidelines apply to whoever receives the call. As soon as it is clear that a caller is making a threat let him/her finish their message without interruption.

Make sure that you write the message down exactly as it is given and try to get some clues on the caller such as;

- Male or female, young or old.
- Was a code word used – if so what was it?
- Conditions which may be affecting the speech such as anger, drunkenness, excitement or incoherence.
- Peculiarities of speech such as accent (foreign?), stutter tone or pitch.
- Any noises in the background – traffic, machinery, music. If a response is required then keep it brief.

When the caller has given the message try to keep him/her in conversation and if possible ask where the device has been placed, at what time is it likely to explode, when was it placed and why etc. The

more information that you can obtain from the caller the more help it will be in dealing with the incident.

A form "Actions to be taken on receipt of a bomb threat" is at Appendix B

Actions for staff

- Stay calm and listen carefully.
- If practical, keep the caller talking and alert a colleague to dial 999.
- Have immediate access to the bomb threat checklist and the key information that should be recorded
- Try to obtain as much information as possible and ask the caller to be precise about the location and timing of the alleged bomb(s) or device(s). Ask the caller who they represent and if they are inclined to talk, keep them talking.
- Note the number of the incoming call, if displayed, from the automatic number display (or use 1471 after the call has ended in case the callers number is recorded)
- If the threat is a recorded message, write down as much detail as possible and retain for the police to secure
- If the threat is received via text message, do not reply to, forward or delete the message; note the number of the sender and follow police advice
- Ensure staff know who to contact in your organisation upon receipt of the threat, e.g. building security/senior manager, as they will need to make an assessment of the threat

Assessing the credibility of bomb threats

Evaluating the credibility of a threat is a critical task, particularly if the attack being threatened is imminent. Short-notice threats are a tactic used to place additional pressure on decision makers, so the better prepared you are, the quicker the police response is likely to be. Police will assess the threat and if specific intelligence is known, will give risk management advice accordingly. However, in the absence of detailed information or specific intelligence, it will be necessary for you to consider a number of factors relevant to your decision-making process:

- Is the threat part of a series? If so, what has happened elsewhere or previously?
- Can the location of the claimed bomb(s) be known with precision? If so, is a bomb visible at the location identified? Has a report of suspicious behaviour been received? Do you have CCTV coverage at/near the location specified?
- If a suspicious item is identified can anyone account for its presence? Are bomb-like characteristics visible? (e.g. wiring or a power source). Was the item located after suspicious activity was noted?
- Considering the hoaxer's desire to influence behaviour as a form of social engineering, is there any good reason to believe their words or follow any instructions they give?
- If the threat is imprecise, could an external evacuation inadvertently move people closer to the hazard specified or to other forms of physical attack, e.g. the possibility of a vehicle as a weapon or knife attack?
-

Actions to consider

Responsibility for the initial decision making remains with the management of the location being threatened and must form part of an inclusive process for managing risk. As already noted, all bomb threats should be reported to the police and their subsequent advice followed. Police will assess the credibility of the threat not just to the building and the people within it, but also to the surrounding

area. This will be done at the earliest opportunity, followed by the provision of appropriate guidance, which may inform your further options. However, do not delay your decision making process waiting for the arrival of police. It is essential that appropriate plans exist and are tested; they should be event and location specific, and accommodate foreseeable variables.

Checking your venue for suspicious items – search considerations

Regular searches i.e. systematic checks of your establishment, proportionate to the foreseeable and plausible risks, will enhance a good security culture and reduce the possibility of an unattended/suspicious item being placed, or remaining unnoticed for long periods. Additionally, if you receive a bomb threat - depending upon how credible it is - you may decide to conduct a 'search' to establish that no such item is in place.

To that end:

- Ensure plans are in place to carry out an effective search in response to a bomb threat
- Identify who in your venue will coordinate and take responsibility for conducting searches
- Initiate a search by messaging over a public address system (coded messages avoid unnecessary disruption and alarm), by text message, personal radio or by telephone cascade
- Divide your venue into areas of a manageable size for 1 or 2 searchers; ideally staff should follow a search plan and search in pairs to ensure the area is covered effectively
- Ensure those conducting searches are familiar with their areas of responsibility; those who regularly work in an area are best placed to spot unusual or suspicious items
- Focus on areas that are open to the public; enclosed areas (e.g. cloakrooms, stairs, corridors, lifts etc.) evacuation routes and assembly points, car parks, other external areas such as goods or loading bays
- Develop appropriate techniques for staff to be able to routinely search public areas without alarming any visitors or customers present
- Ensure all visitors know who to report a suspicious/unattended item to, and have the confidence to report suspicious behaviour
- Under no circumstances should any item assessed as suspicious be touched or moved in any way. Once an item is declared suspicious by a competent person, commence evacuation immediately and dial 999.
-

Familiarising through testing and exercising will increase the likelihood of an effective response to an evacuation and aid the decision making process when not to evacuate/invacuate.

Delivered Items

By the very nature of the event it necessitates receiving a wide variety of deliveries.

Delivered items, which include letters, parcels, packages and anything delivered by post or courier, has been a commonly used terrorist device. Delivered items may be explosive or incendiary (the two most likely kinds), or chemical, biological or radiological (CBR). Anyone receiving a suspicious delivery is unlikely to know which type it is.

Delivered items come in a variety of shapes and sizes. Incendiary devices have been located in cigarette packets, tape cassettes, briefcases or sports bags. There can be no exact descriptions of what to expect.

The traditional postal device takes many forms, parcels, padded "jiffy bags", or envelopes of any shape or size. They may be delivered by hand or via a courier as well as through the post.

Indicators to Suspicious Deliveries/Mail

- It is unexpected or of unusual origin or from an unfamiliar sender. There is no return address or the address cannot be verified.
- It is poorly or inaccurately addressed.
- The address has been printed unevenly or in an unusual way. The writing is in an unfamiliar or unusual style.
- There are unusual postmarks or postage paid marks.
- It seems unusually heavy for its size.
- It is marked 'personal' or 'confidential'.
- It is oddly shaped or lopsided.
- There is an unusual smell but be aware that homemade explosives might not smell of traditional almonds or marzipan and might smell otherwise
- Staining on the packaging or liquid leaks
- There is an additional inner envelope, and it is tightly taped or tied.
- It has possibly an unusual number of postage stamps (the sender will be unlikely to have access to company post franking systems)
- Markings to indicate the recipient should open the item in a particular way or at one end.

SUSPICIOUS PACKAGES OR BAGS

Good housekeeping improves the ambience of an event and reduces the opportunity for placing suspicious items or bags and helps to deal with false alarms and hoaxes. Terrorists in particular have a long history of leaving hand carried devices, holdalls, packages and so on, in public places or places to which access is simple.

If in any doubt leave any suspicious item in place, obtain assistance and do not touch the object.

Staff are the most valuable asset and their protection is paramount. They are also one of the best sources of protection. Staff should know their own office, work environment and parking area intimately. All staff should keep a sharp lookout for unusual behaviour or items out of place and have the support of managers to report things and know that their reports will be taken seriously and recognised as a positive contribution to the business.

In a terrorist context staff should be particularly vigilant if they see anyone placing, rather than dropping, a packet or bag in an unusual place, or in a fairly inaccessible area out of sight. Devices will be carefully but not elaborately concealed.

It is highly likely that during your event you will encounter unattended bags, holdalls etc. many, if not all, of these will be items that have been accidentally lost or misplaced; however, in the current climate all should be treated as suspect until proved otherwise.

When dealing with an abandoned item the H.O.T. principles will be applied in order to assist in deciding whether the item should be regarded as suspicious and therefore the response would be upgraded.

HOT Principles

Consider using the below when dealing with an unattended bag or item when there is no other information or intelligence to suggest that it is suspicious.

H – Hidden
Hidden deliberately? Has a deliberate attempt been made to hide the item from view? Is it in a place where accidental discovery is unlikely?

O – Obvious
Obviously suspicious (does it look like a bomb, are there batteries/wires showing etc)? Why has it been abandoned? Has it been found after a suspicious event or report of someone acting furtively?

T – Typical
Typical of what you would expect to find at location. Lots of the crowd will have bags. Can anyone who knows the area well confirm its staus?

Any report of an abandoned/unattended item should be dealt with by event control who will deploy a member of security response. Event Control should keep a full log of the response and outcome.

Action to be taken upon declaration of any suspicious item

When dealing with **suspicious items** apply the 4 Cs protocol:

Confirm, Clear, Communicate and Control.

CONFIRM whether or not the item exhibits recognisably suspicious characteristics.

CLEAR the immediate area

- Do not touch it
- Take charge and move people away to a safe distance. Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out.
- Keep yourself and other people out of line of site of the item. It is a broad rule, but generally if you cannot see the item then you are better protected from it.
- Think about what you can hide behind. Pick something substantial and keep away from glass such as windows and skylights.
- Cordon off the area.

COMMUNICATE – Call 999

- inform your control room and/or supervisor
- Do not use radios or mobile phones within 15 metres.
- **Remember:** If you think it's suspicious, say something

CONTROL access to the cordoned area

Maintain control of the area; members of the public should not be able to approach the area until it is deemed safe, try and keep eyewitnesses on hand so they can tell police what they saw

DO NOT USE MOBILE PHONES OR TWO-WAY RADIOS IN THE CLEARED AREA OR WITHIN 15 METERS OF THE SUSPECT ITEM

Please be vigilant at all times and keep a sharp look out for unusual behaviour or items out of place.

SEARCHING PREMISES AND ZONED SEARCH PROCEDURES

A search may be initiated in response to a specific threat. Bombs and incendiary devices are disguised in many ways. Searchers do not have to be expert in explosive devices. They are looking for anything:

- That should not be there
- That cannot be accounted for
- That is out of place.

Upon receipt of a threat a search should be implemented immediately and the police should be informed. Whilst the search is being carried out the police will be checking for an assessment of the credibility of the threat.

Staff nominated to carry out a search do not need to have expertise in explosives or other types of device but they must be familiar with the place they are searching.

They are looking for any items that should not be there, that cannot be accounted for and items that are out of place.

Following receipt of a bomb threat the police will not normally search premises. They are not familiar with the premises and layout, and will not be aware of what should be there and what is out of place. They cannot therefore search as quickly and as thoroughly as staff that work there all the time. The objective is to make sure that the whole building or area is checked as quickly and effectively as possible. Ideally, searchers should search in pairs to ensure searching is systematic and thorough.

Areas which will be used as safe areas or evacuation assembly areas, together with those areas where the greater number of the public, visitors or staff are likely to be vulnerable should be searched first. Public areas to which anyone has easy access should also have priority. Car parks, service yards, the outside area and perimeter should not be overlooked.

The searcher who finds a suspicious item must not move or interfere with it in anyway but inform Event Control.

- Do not touch or move the item
- Move everyone away to a safe distance
- Prevent others from approaching
- Use hand held radios or mobile phones away from the immediate vicinity of a suspect item, remaining out of line of sight and behind hard cover
- Inform Event Control giving as much information as possible
- The person finding the device must remain on hand to brief the police on the exact location and description.

HOSTILE VEHICLE INCURSION

Most recent terrorist attacks in the UK and mainland Europe have moved away from sophisticated attacks using explosive devices and now use more readily available everyday items, enabling an attack to be more spontaneous. A preferred weapon is now a motor vehicle.

The possibility of an attack using a motor vehicle at an event could be from a vehicle brought to the event by a hostile person, who then gains access to the public areas to perform their attack. A second, more spontaneous, option would be for a hostile to use a vehicle that is already on the site.

If you are considering the use of physical measures to prevent hostile vehicles entering the event you are strongly advised to contact police and ask for expert advice from a specialist officer such as a Counter Terrorism Security Advisor (CTSA) or Counter Terrorism Security Co-ordinator (CT-SecCo).

HOSTILE PERSON INCURSION

Recent terrorist attacks have also involved intent to do harm with firearms or bladed weapons. The procedures outlined earlier in this plan relating to identifying anyone acting suspiciously may deter potential attackers but, if an armed individual is reported, then the following procedures should apply.

- All personnel should be reminded of “Run, Hide, Tell”.
- Inform Police
- Inform Security staff
- Consider Dynamic Lockdown
- Inform medical provider in case of mass casualties
- Inform Stewards / Traffic Management contractors to expect arrival of emergency services

RUN, HIDE, TELL

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, but don’t let their indecision slow you down.
- Leave belongings behind.
- Do not attempt to film the incident. Run.

HIDE

- If you cannot 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. You must still hide, even If you are behind a locked door.
- 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 and turn off vibrate
- Lock/barricade yourself in
- Move away from the door

TELL

Call 999 – What do the police need to know? If you cannot speak or make a noise, listen to the instructions given to you by the call taker:

- Nature of the Incident - What is happening?
- Location - where is the incident taking place? Give an address or general location
- Suspects – 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

DYNAMIC LOCKDOWN PROCEDURE

There may be circumstances where an event may have to implement a "lockdown" procedure.

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).

Due to the nature of the site it may not be possible to physically achieve complete lockdown.

Lockdown may also be implemented when there is no incident on the site, the incident may be nearby or information has been received that a threat is on its way to the site and lockdown is necessary to protect those already at the event.

https://www.cpni.gov.uk/marauding-terrorist-attacks-1

NATIONAL MOVE TO CRITICAL

Following a change of the threat level to CRITICAL there are a number of options you may wish to consider.

Threat Level Definitions

There are five levels of threat which are defined below:

CRITICAL	AN ATTACK IS HIGHLY LIKELY IN THE NEAR FUTURE
SEVERE	AN ATTACK IS HIGHLY LIKELY
SUBSTANTIAL	AN ATTACK IS LIKELY
MODERATE	AN ATTACK IS POSSIBLE, BUT NOT LIKELY
LOW	AN ATTACK IS HIGHLY UNLIKELY

Current threat levels and further information can be obtained from Threat Levels | MI5 - The Security Service

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.

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

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 arrangement 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.

Staff Vigilance

- 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?
- Disrupting hostile reconnaissance: Ensure staff understand how to identify suspicious behaviour (Do you have a challenge culture?)
- Suspicious Items: Ensure staff understand how to respond to suspicious items. Do staff know the HOT principles?
- Where entry is restricted, check the visitors identification prior to allowing access to the site

Free Counter Terrorism Training

Under the national Action Counters Terrorism (ACT) programme (previously known as Project Griffin and Argus) you and your staff can obtain free training in all the topics described in this document. The sessions can be via a Police or County Council trained expert to a group by means of a PowerPoint, film and talk presentation or via registered access to an E-Learning programme.

Local Counter Terror Security Advisors can also train a range of SCaN products free of charge.

For further details email ctsa@lincs.police.uk

APPENDIX A - SUSPICIOUS BEHAVIOUR REPORTING FORM

Inform your Security Manager and the incident must be reported via 101 or 999

Date:	**Time:**	**Location:**

CCTV / OTHER IMAGES:

Yes		**No**		**No of persons involved:**	

ACTIVITY – WHY IS THE BEHAVIOUR SUSPICIOUS?
(photography, video, extended observation, accessed restricted area etc.)

PERSON

Description		
Gender	**Ethnicity**	**Facial features**
Clothes / Footwear	**Build**	**Hair style/colour**

Height approx	Identifying features (e.g. Tattoos/scars/facial hair, birthmarks, piercings etc.)	Speech/accent/wording/phases

Equipment carried (Camera/bag, etc.)	Seen before?	Mode of travel (on foot/tram/train/car etc)

VEHICLE DETAILS

Vehicle vrm:	Colour:	Make / Model:

Further info: Stickers/damage/body kit, etc.	

Was the person challenged? (If so what was their response or comments)

Additional information:

APPENDIX B - ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

This checklist is designed to help staff deal with a telephoned bomb threat effectively and to record the necessary information

Protective Marking: Restricted when Completed

1 Remain calm and talk to the caller
2 Note the caller's number if displayed on your phone
3 If the threat has been sent via email or social media see appropriate section below
4 If you are able to, record the call
5 Write down the exact wording of the threat:

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

ASK THESE QUSTIONS AND RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. Where exactly is the bomb right now?
2. When is it going to explode?
3. What does it look like?
4. What does the bomb contain?
5. How will it be detonated?
6. Did you place the bomb? If not you, who did?
7. What is your name?
8. What is your address?
9. What is your telephone number?

10. Do you represent a group or are you acting alone?
11. Why have you placed the bomb?
Record time call completed:

INFORM SECURITY OR COORDINATING MANAGER
DIAL 999 AND INFORM POLICE

Name and telephone number of person informed:	**Time informed:**

This part should be completed once the caller has hung up and police/ building security/ coordinating manager have all been informed

Date and time of call:	Duration of call:	The telephone number that received the call:

ABOUT THE CALLER:	Male	Female	Nationality?	Age?

THREAT LANGUAGE:	Well-spoken	Irrational	Taped	Foul	Incoherent

CALLER'S VOICE:		Calm	Crying	Clearing throat	Angry	Nasal
Slurred	Excited	Stutter	Disguised	Slow	Lisp	*Accent
Rapid	Deep	Familiar	Laughter	Hoarse	**Other** (please specify)	

*What accent?

If the voice sounded familiar, who did it sound like?

BACKGROUND SOUNDS:	Street noises	House noises	Animal noises	Crockery	Motor

Clear	Voice	Static	PA system	Booth	Music
Factory machinery		Office machinery		**Other** (please specify)	

Protective Marking: Restricted when Completed

REMARKS:		
ADDITIONAL NOTES:		
Signature:	Print Name:	Date:

FOR FURTHER INFORMATION AND GUIDANCE:

Please see

www.nactso.gov.uk
www.cpni.gov.uk
NPCC Stay Safe Guidance

Know what to do and prepare yourself with CitizenAID: **https://www.citizenaid.org/citizenaid**

Action Counters Terrorism - ACT NOW: gov.uk/ACT