Counter Terrorism Protective Security Advice

for Stadia and Arenas

ASSOCIATION OF CHIEF POLICE OFFICERS

POLICE SCOTLAND

produced by

NaCTSO

National Counter Terrorism Security Office

contents

one introduction

This guide is intended to give protective security advice to those who are responsible for stadium and arena security, irrespective of size and capacity and is not specific to any particular sport or event. It is aimed at those stadia and arenas that are seeking to reduce the risk of a terrorist attack, or limit the damage terrorism might cause.

It is accepted that there is no such concept as absolute safety or absolute security in combating the threat of terrorism but it is possible through the use of this guidance to reduce the risk to as low as reasonably practicable.

The bomb attacks in London in July 2005 demonstrated that the threat from terrorism is real and serious. Although actual attacks have so far been infrequent, it is possible that you may find your stadium caught up in a terrorist incident. This might include having to deal with a bomb threat or with suspect items sent through the post or left in the Stadium. In a worst case scenario, you or your staff could be directly affected by a terrorist attack.

Terrorism can come in many forms, not just a physical attack. It can take the form of attacks on vital information or communication systems, causing disruption and economic damage. Some attacks are easier to carry out if the terrorist is assisted by an 'insider' or by someone with specialist knowledge or access. Terrorism also includes acts and hoaxes designed to frighten and intimidate. These have previously been targeted at stadia.

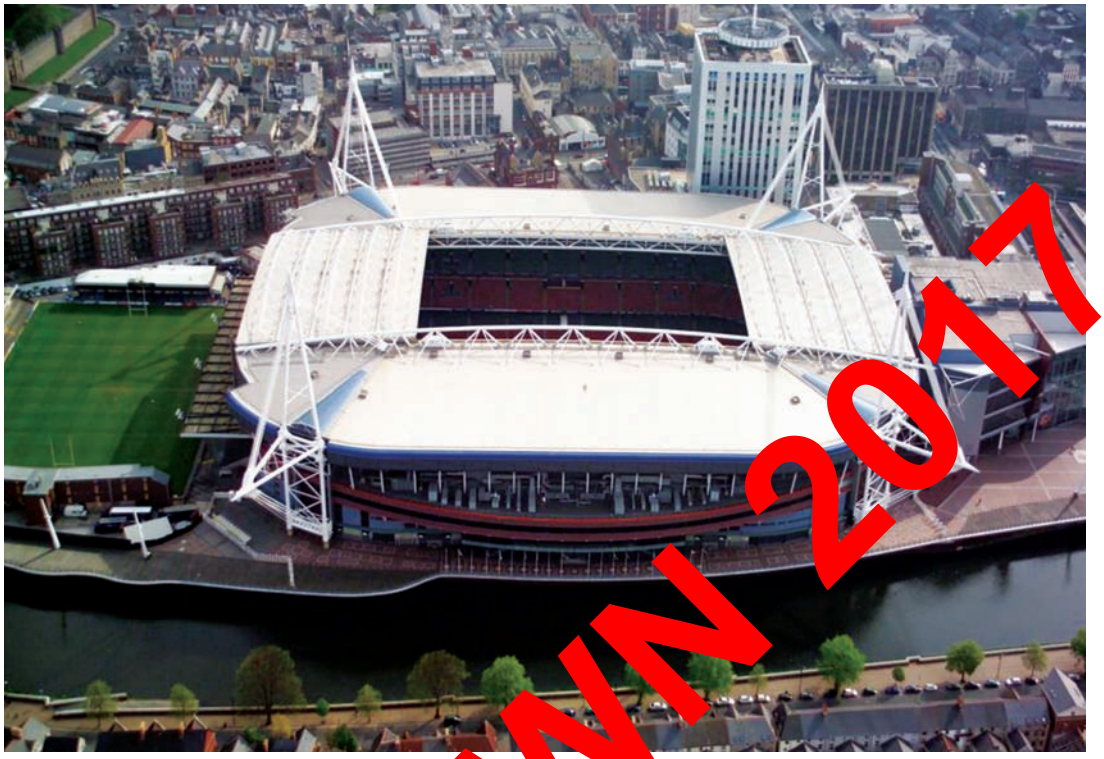
> It is worth remembering that measures you may consider for countering terrorism will also work against other threats, such as theft and burglary. Any extra measures that are considered should integrate wherever possible with existing security.

There are three strong business reasons why your stadium should plan to deter such acts, or at least to minimise their impact. They are:

- **Legal obligations.** In the event of an incident, your written risk assessments and plans may come under scrutiny. Health & Safety at Work regulations and where relevant the Safety at Sports Grounds legislation put the responsibility on the owner or lessee of the stadium to provide a duty of care and to ensure the reasonable safety of everyone who visits their stadium. Although the police, stadium regulatory bodies and other agencies can offer advice, it is up to the owner or lessee of the stadium to seek out and act upon that advice. In any subsequent inquiries or court proceedings, you would need to show that you took the relevant legislation into account.
- **Business continuity.** Ensuring that your stadium and organisation is able to cope with an incident or attack and return to normality as soon as possible. An attack on a crucial contractor or supplier can also impact on business continuity. This is particularly important for smaller stadia that may not have the resources to withstand even a few days of financial loss.
- **Loss of reputation**

In addition, make sure that your organisation has adequate insurance to cover terrorist threats – consult your insurance company or broker.
There is limited value in safeguarding your own business premises in isolation. Take into account your neighbours' plans and those of the emergency services.

Do you know who your neighbours are and the nature of their business and could an incident at their premises affect your stadium operation?



A number of organisations have adopted good practice to enhance the protective security measures at their stadiums on both event and non event days. This document compliments such good practice measures.

Being security minded and being prepared reassures your customers and staff that you are taking security issues seriously.

This document is not 'sport specific' and recognises that all stadia and arenas are different; irrespective of the sport or event that takes place. It is also recognised that some of the guidance included in this document may have already been introduced by various stadia.

For specific advice relating to your stadium, contact the nationwide network of specialist police advisers known as Counter Terrorism Security Advisors (CTSAs) through your local police service. Their work is co-ordinated by the National Counter Terrorism Security Office (NaCTSO).

REMEMBER!
The Hillsborough Stadium disaster in 1989 taught us a critical lesson. Safety must always have priority over security.

It is essential that all the work you undertake on protective security is undertaken in partnership with the police and your neighbours, if your stadium is to be secure.

As well as safeguarding your own business, the steps you take can make an important contribution to preventing and detecting terrorists.

two managing the risks

Managing the risk of terrorism is only one part of stadium managements' responsibility when preparing contingency plans in response to any incident occurring at a stadium which might prejudice public safety or disrupt normal operations.

Management already have a responsibility under Health and Safety Regulations and under the Safety Certificate issued under the Safety at Sports Grounds Act 1975 and/or the Fire Safety and Safety of Places of Sport Act 1987.

See Guide to Safety at Sports Grounds www.safetyatsportsgrounds.org.uk

At all grounds designated by the Secretary of State or which have regulated stands, the local authority will issue a safety certificate. This lays down terms and conditions with which the stadium / arena must comply in order to admit a specified number of spectators. The conditions will include the production of contingency plans.

The local authority will monitor and enforce the safety certificate in a number of cases on the advice of the safety advisory group.

With regard to protective security, the best way to manage the hazards and risks to your stadium is to start by identifying the threats and vulnerabilities.

This will help you to decide:

- What security improvements you need to make
- What type of security and contingency plans you need to develop.

For some stadia, simple good practice - coupled with vigilance and well practiced contingency arrangements - may be all that is necessary.

If, however, you assess that there is a risk, you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable.

The following diagram illustrates a typical risk management cycle:

Step One: Identify the threats.

Understanding the terrorist's intentions and capabilities - what they might do and how they might do it - is crucial to assessing threat. Ask yourself the following questions:

- What can be learnt from the government and media about the current security climate, or about recent terrorist activities? Visit www.mi5.gov.uk
- Is there anything about your stadium, staff or activities that would particularly attract a terrorist attack?
- Is there an association with high profile individuals or organisations which might be terrorist targets?
- Do you have procedures in place and available for deployment on occasions when VIPs attend your stadium?
- Does your location mean that you may suffer business disruption from an attack or other incident to a high risk neighbour?
- What can your local Police Service tell you about crime and other problems in your area?
- Is there any aspect of your business or activities that terrorists might wish to exploit to aid their work, e.g. plans, technical expertise or unauthorised access on event and non-event days?
- Do you communicate the threat to your staff?

Step Two: Decide what you need to protect & identify your vulnerabilities.

Your priorities for protection should fall under the following categories:

- People (staff, including playing staff, contractors, spectators, visitors)
- Physical assets (the fabric of your stadium / arena and its contents)
- Information (electronic and non-electronic data)
- Processes (supply chain, procedures).

You should already know what is important to your business. It may be something tangible - for example, the data suite where all your transactions are recorded, the IT system or a piece of equipment that is essential to keep your business running. Or it may be less tangible, such as continued access for the public.

You may already have plans in place to safeguard your most important assets from other threats. For example:

- You should already have contingency plans to deal with any incident likely to prejudice public safety or disrupt the normal operation of the stadium e.g. fire and crime
- You should have procedures for assessing the reliability and integrity of those you wish to employ
- You may have taken steps to protect your IT systems from viruses and hackers; these systems should be continuously updated
- You should have measures in place to limit individuals' access to parts of the stadium and incorporate appropriate access control measures.

If you have reason to believe that you are at greater risk of attack because of the nature of

your business or the location of your premises, consider what others could find out about your vulnerabilities, such as:

- What information about you is in the public domain, e.g. on the internet or in public documents?
- What published facts point to installations or services that are vital to the continuation of your business?

As with Step One, consider whether there is an aspect of your business or activities that terrorists might want to exploit to aid or finance their work. If there are, how stringent are your checks on the people you recruit or on your contract personnel? Are your staff security conscious?

How good are your staff at spotting unusual activity? (See hostile reconnaissance on page 15).

Step Three: Identify measures to reduce risk

You are unlikely to be able to eliminate risk altogether, therefore you should identify the most appropriate measures to reduce risk to as low as reasonably practicable. You need to protect those aspects of your business that are critical, which will always include your staff. This involves:

- Physical security
- Managing staff securely (i.e. good personnel practices) and
- Information security.

There is little point investing in costly security measures if they can be easily undermined by a disaffected insider, or by a lax recruitment process.

Remember, TERRORISM IS A CRIME. Many of the security precautions typically used to deter criminals are also effective against terrorists.

This means that you may already have a good security regime on which you can build. Before you invest in additional security measures, review what is already in place, including permanent security staff and stewards employed on the day of an event.

Staff may be unaware of existing security measures, or may have developed habits to circumvent them. Simply reinforcing good basic security practices and regularly reviewing them will bring benefits at negligible cost.

Step Four: Review your security measures & rehearse and review security and contingency plans.

You should conduct regular reviews and exercises of your plans to ensure that they remain effective and workable and up to date. You should be aware of the need to modify them to take into account any changes in your stadium (e.g. new building work, changes to personnel, information and communication systems and revised health and safety issues).

Rehearsals and exercises should wherever possible, be conducted in conjunction with the emergency services and local authority.

Make sure that your staff understand and accept the need for security measures and that security is seen as part of everyone's responsibility, not merely something for security experts or professionals. Make it easy for people to raise concerns or report observations.

IT SHOULD BE REMEMBERED THAT THE GREATEST RISK TO ANY ORGANISATION IS COMPLACENCY.

three security planning

It is recognised that for the majority of stadia responsibility for the implementation of protective security measures following a vulnerability and risk assessment will fall on the Stadium Safety Officer / Designated Person.

The Stadium Safety Officer / Designated Person must have sufficient authority to direct the action taken in response to a security threat and have direct access to the board of directors.

He or she must be involved in the planning and design of the stadium's interior security, access control etc, so that the terrorist dimension is taken into account. The Safety Officer / Designated Person must similarly be consulted over any new building or refurbishment work, so that counter-terrorism specifications, e.g. concerning glazing and physical barriers can be factored in, taking into account any planning, safety and fire regulations.

The Safety Officer / Designated Person at most stadia should already have responsibility for most if not all of the following key areas:

- The production of the security plan based on the risk assessment
- The formulation and maintenance of search plans
- The formulation and maintenance of contingency plans dealing with bomb threats, suspect packages and evacuation
- Liaising with the police, other emergency services and local authorities
- Arranging staff training, including their own deputies and conducting briefings / debriefings
- Conducting regular reviews of the plans.

For independent and impartial counter terrorism advice and guidance that is site specific, the Safety Officer / Designated Person should establish contact with the local police Counter Terrorism Security Advisor (CTSA). Most UK Police Forces have at least two CTSAs.

Your CTSA can:

- Help you assess the threat, both generally and specifically
- Give advice on physical security equipment and its particular application to the methods used by terrorists; your CTSA will be able to comment on its effectiveness as a deterrent, as protection and as an aid to post-incident investigation
- Give advice on local installers of equipment
- Offer advice on search plans.

During the development and review of plans it is also advisable to discuss them with other occupants of the stadium (hotels etc) and with neighbours, as well as to consult all the emergency services and your local authority.

Creating your Security Plan

The Safety Officer / Designated Person should aim to produce a plan that has been fully exercised, and which is regularly audited to ensure that it is still current and workable.

When creating your security plan, consider the following:

- Details of all the protective security measures to be implemented, covering physical, information and personnel security
- Instructions on how to respond to a threat (e.g. telephoned bomb threat)
- Instructions on how to respond to the discovery of a suspicious item or event
- A search plan
- Evacuation plans and details on securing the stadium in the event of a full evacuation
- Your business continuity plan
- A communications and media strategy which includes handling enquiries from concerned family and friends.

Safety Officers / Designated Persons should also be familiar with the advice contained in the Safety at Sports Grounds guidance. See www.safetyatsportsgrounds.org.uk

Your planning should incorporate the seven key instructions applicable to most incidents:

1. Do not touch suspicious items
2. Move away to a safe distance
3. Prevent others from approaching
4. Communicate safely to staff, visitors and the public
5. Use hand-held radios or mobile phones away from the immediate vicinity of a suspect item
6. Notify the police
7. Ensure that whoever found the item or witnessed the incident remains on hand to brief the police.

Effective security plans are simple, clear and flexible, but must be compatible with existing plans, e.g. evacuation plans. Everyone must be clear about what they need to do in a particular incident. Once made, your plans must be followed.

four physical security

Physical security is important in protecting against a range of threats and vulnerabilities, including terrorism.

Put in place security measures to remove or reduce your vulnerabilities to as low as reasonably practicable bearing in mind the need to consider safety as a priority at all times. Security measures must not compromise spectator safety.

Your risk assessment will determine which measures you should adopt, but they range from basic good housekeeping (keeping communal areas such as reception clear and tidy) through CCTV, intruder alarms, computer security and lighting, to specialist solutions such as mail scanning equipment.

Specialist solutions, in particular, should be based on a thorough assessment - not least because you might otherwise invest in equipment which is ineffective, unnecessary and expensive.

Successful security measures require:

- The support of senior management
- Staff awareness of the measures and their responsibility in making them work
- Someone within your organisation having responsibility for security.

Action you should consider

Contact your Counter Terrorism Security Advisor (CTSA) through your local police force at the start of the process. As well as advising you on physical security, they can direct you to professional bodies that regulate and oversee reputable suppliers.

Remember too that you will need to ensure that all necessary regulations are met, such as local planning permission, building consents, Health and Safety and fire prevention requirements.

Plan carefully – as this can help keep costs down. Whilst it is important not to delay the introduction of necessary equipment or procedures, costs may be reduced if new changes coincide with new building or refurbishment work.

Security awareness

The vigilance of your staff (including stewards, cleaning, maintenance and event day staff) is essential to your protective measures. They will know their own work areas or offices very well and should be encouraged to be alert to unusual behaviour or items out of place.

They must have the confidence to report any suspicions, knowing that reports - including false alarms - will be taken seriously and regarded as a contribution to the safe running of the stadium.

Training is therefore particularly important. Staff should be briefed to look out for packages, bags or other items in odd places, carefully placed (rather than dropped) items in rubbish bins and unusual interest shown by strangers in less accessible places. See hostile reconnaissance on page 45.

Access control

An efficient reception area is essential to controlling access, with side and rear entrances denied to all but authorised people.

Keep access points to a minimum and make sure the boundary between public and private areas of your building is secure and clearly signed. Invest in good quality access controls such as magnetic swipe identification cards or proximity card systems. See Access Control Guidance on page 17.

Security passes

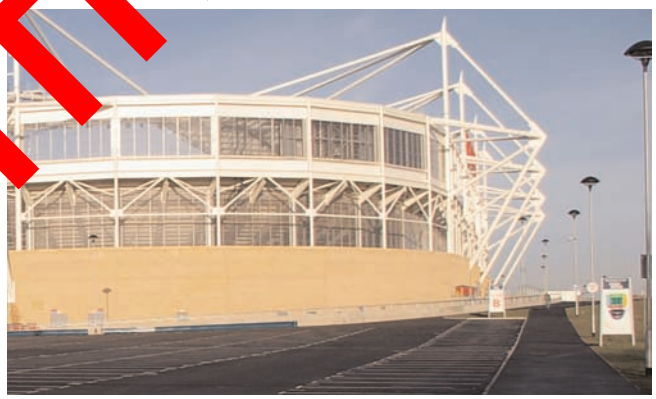
If a staff pass system is in place, insist that staff wear passes at all times and that their issuing is strictly controlled and regularly reviewed. Visitors should be escorted and should wear clearly marked temporary passes, which must be returned on leaving. Anyone not displaying security passes should either be challenged or reported immediately to security or management. Consider introducing a pass system if you do not have one already.

Screening

The random screening of hand baggage is a significant deterrent and you have the right to refuse entry to anyone who refuses to allow you to search their possessions. However, body searches may be carried out only with the agreement of the person being searched. Refusal to allow a body search could be regarded as good grounds to refuse admission to the stadium.

Routine searching and patrolling of premises represents another level of screening; covering both internal and external areas. Keep patrols regular, though not too predictable (i.e. every hour on the hour). See Search Planning on page 25.

Traffic and parking controls



If you believe you might be at risk from a vehicle bomb, the basic principle is to keep all vehicles at a safe distance. Those requiring essential access should be identified in advance and checked before being allowed through. If possible, you should ensure that you have proper access control, careful landscaping, traffic-calming measures and robust, well-lit barriers or bollards. Ideally, keep non-essential vehicles at least 30 metres from your building.

For site specific advice and guidance you should contact your local police Counter Terrorism Security Advisor (CTSA).

See also Vehicle Borne Improvised Explosive Devices on page 37.

Doors and windows

Good quality doors and windows are essential to ensure building security. External doors should be strong, well-lit and fitted with good quality locks. Consideration should also be given to alarms. Remember that glazed doors are only as strong as their weakest point, which may be the glazing.

All accessible windows should have good quality key operated locks.

Many injuries in urban terrorist attacks are caused by flying glass, especially in modern buildings and glazing protection is an important casualty reduction measure. Extensive research has been carried out on the effects of blast on glass. There are technologies that minimise shattering and casualties, as well as the costs of re-occupation. Anti-shatter film, which holds fragmented pieces of glass together, offers a relatively cheap and rapid improvement to existing glazing. If you are installing new windows, consider laminated glass but before undertaking any improvements seek specialist advice through your police CTSA.

Integrated security systems

Intruder alarms, CCTV and lighting are commonly used to deter crime, detect offenders and delay their actions. All these systems must be integrated so that they work together in an effective and co-ordinated manner.

Intrusion detection technology can play an important role in an integrated security system; it is as much a deterrent as a means of protection. If police response to any alarm is required, your system must be compliant with the Association of Chief Police Officers' (ACPO) security system policy. See www.securedbydesign.com and www.acpo.police.uk For further information, contact the Alarms Administration Office at your local police headquarters.

The alarm system within stadia and areas within Scotland should be compliant with **the requirements of** www.scotland.police.uk Alternatively advice can be obtained by local CTSA officers located within local police offices.

Using CCTV can help clarify whether a security alert is real and is often vital in post-incident investigations, but only if the images are good enough to identify what happened and be used in court.

External lighting provides an obvious means of deterrence as well as detection, but take into account the impact of additional lighting on neighbours. If it is carefully designed and used, external lighting will help security staff and improve the capabilities of CCTV systems.

Remember however, that CCTV is only effective if it is properly monitored and maintained.

CCTV guidance on page 19.

WITHDRAWN 2017

five good housekeeping

Basic good housekeeping reduces the opportunity for planting suspect packages or bags and helps to deal with false alarms and hoaxes.

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

- Avoid the use of litter bins around the stadium if possible, (but if you do th ensure that there is additional ar prompt cleaning)
- The use of clear bags for waste disposal is an alternative as it provides easier opportunity for staff to conduct an initial examination for suspect packages
- Review the use and security of compactors, wheelie bins and metal bins to store rubbish within stadiums and arenas or next to structures and do not place any bins next to or near any glazing
- Keep all public and communal areas – exits, entrances, reception areas, stairs, halls, lavatories, washrooms – clean and tidy
- Keep the furniture in such areas to a minimum – ensuring that there is little opportunity to hide devices
- Lock unoccupied offices, rooms and storerooms
- Ensure that everything has a place and that things are returned to that place
- Put plastic seals on maintenance hatches
- Keep external areas as clean and tidy as possible
- All stadia and arenas should have in place an agreed protocol for the security of outside broadcast companies vehicles, equipment and personnel as well as contractors vehicles and waste collection services. The vehicle registration mark (VRM) of each vehicle and its occupants should be known to stadium security in advance
- Stadiums using nearby facilities, such as local schools for parking, must ensure that adequate stewarding and security is provided at these places
- Arrangements for not receiving post to the stadium/arena on event days
- Cutting all vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any packages.

Additionally consider the following points.

- Ensure that all staff who could conceivably receive a bomb threat are trained in handling procedures or at least have ready access to instructions – and know where these are kept. (See Bomb Threat Checklist)
- Review of current stadium CCTV system to ensure that it has sufficient coverage bo internally and externally
- Stadium management should ensure that Fire Extinguishers are marked as Cl roperty and check that they have not been replaced immediately prior to an event
- Stadium management should identify a secondary secure location fo Co ol Room as part of their normal contingency plans
- Security systems that are reliant on power should have an Un errupted Power Supply (UPS) available and regularly tested.

See Good Practice checklist – Housekeeping in Appendix 'A

six access control

There should be clear demarcation between public and private areas, with appropriate access control measures into and out of the private side. This relates to private areas within the stadium not entry gates or turnstiles for spectators on event days.

Risk assessment

Refer to 'managing the risks' on page 5 and de[cide] the level of security you require before planni[ng] your Access Control system. Take into ac[count] special features you may require.

Appearance

Your Access Control system is often the first impression of security made on vi[sitors] to your stadium.

Ease of access

Examine the layout of your system. Do your entry and exit proced[ures] a[llow] legitimate users to pass without undue effort and delay?

Training

Are your staff fully aware of the role and operati[on] of your Ac[cess] Control system? Your installer should provide adequate system training.

System maintenance

Your installer should supply all releva[nt] syst[em] documentation, e.g. log books and service schedules. Are you aware of the actions [re]quired on system breakdown? Do you have a satisfactory system maintenan[ce] agre[ement in] place?

Interaction

Your Access Control syste[m] may s[upp]lement other security measures. Consider system compatibility.

Compliance

Are you compli[ant] with:

Equa[lity] Act 2010
The Hu[man] Ri[ghts] Act 1998
[Health] and Safety at Work Act 1974
The Data Protection Act 1998
Regulatory Reform (Fire Safety) Order 2005

Objectives

Are your security objectives being met? If necessary, carry out a further risk assessment and address any shortcomings accordingly.

Access control is only one important element of your overall security system.

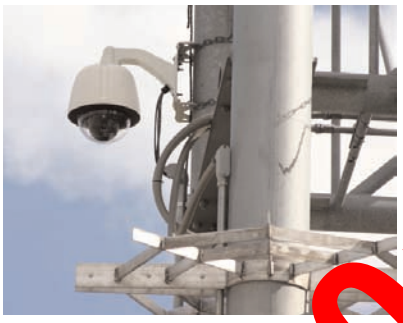
Remember!

Whether driving a lorry or carrying explosives, a terrorist needs physical access in order to reach the intended target.

See Good Practice Checklist – Access Control & Visitors in Appendix 'B'

seven cctv guidance

Ask yourself the following questions:



- Is your CCTV system currently achieving what you require it to do? Do you need it to confirm alarms, detect intruders through gates or over fences and produce images of evidential quality?
- Are the CCTV cameras in use for the protective security of your stadium integrated with those used to monitor crowd movement?

The Centre for Applied Science and Technology CAST formerly known as The Ho e Of e Scientific Development Branch (HOSDB), has published many useful documents relati t CCTV, including 'CCTV Operational Requirements Manual' (Ref: 28/09), ' Police Requirements for Digital CCTV Systems' (Ref: 09/05), and 'Performance Tes of CCTV Systems' (Ref: 14/95). 'Performance Testing of CCTV Systems' (Re 'CCTV Control Room Ergonomics' (Ref: 14/98).

CCTV cameras should cover the entrances and exits to your ad d other areas that are critical to the safe management of any event at the sta a l to the security of your business.

Constantly monitor the images captured by your TV or regularly check recordings for suspicious activity ensuring at all time com ce with the Data Protection Act 1998 which should be specified in your CC Data rotec n Policy.

Consider also the following points:

- Ensure the date and time st nps o e sy em are accurate
- Regularly check the qu ity o cordi gs
- Digital CCTV image sho e st ed in accordance with the evidential needs of the Police. Refer to CAST (HO publi ion 09/05 - UK Police Requirements for Digital CCTV Systems.
- Ensure that app riate lighting compliments the system during daytime and darkness ho s
- eep ur re ded images for at least 31 days
- e go quality media and check it regularly by checking that backups are operating correctly.
- e the images recorded are clear – that people and vehicles are clearly identifiable
- Check that the images captured are of the right area
- Implement standard operating procedures, codes of practice and audit trails
- Give consideration to the number of camera images a single CCTV operator can effectively monitor at any one time.

See Good Practice Checklist – CCTV in Appendix 'C'

CCTV Maintenance

CCTV maintenance must be planned and organised in advance and not carried out on an ad-hoc basis. If regular maintenance is not carried out, the system may eventually fail to meet its original Operational Requirement (OR).

What occurs if a system is not maintained?

- The system gets **DIRTY** causing poor usability
- **CONSUMABLES** wear causing poor performance
- Major parts **FAIL**
- **WEATHER** damage can cause incorrect coverage
- **DELIBERATE** damage / environmental changes can go undetected

eight mail handling

Most stadia and arenas receive large amounts of mail and other deliveries and this offers an attractive route into your stadium for terrorists. See guidance at www.cpni.gov.uk

Suspicious Mail

Suspicious mail, which includes parcels, packages and anything delivered by post or courier, has been a commonly used terrorist device. A properly conducted risk assessment should give you a good idea of the likely threat to your organisation and indicate precautions you need to take.

Suspicious mail may be explosive or incendiary (the two most likely kinds), or chemical, biological or radiological. Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality.

A letter bomb will probably have received fairly rough handling in the post and so is unlikely to detonate through being moved, but any attempt at opening it, however slight, may set it off. Unless delivered by courier, it is unlikely to contain a timing device. Letter bombs come in a variety of shapes and sizes; a well-made one will look innocuous but there may be tell-tale signs.

Indicators to Suspicious 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 e.g. incorrect title, spelt wrongly, title but no name, or addressed to an individual no longer with the company
- The address has been printed unevenly or in an unusual way
- The writing is in an unfamiliar foreign style
- There are unusual postmarks or postage paid marks
- A Jiffy bag, or similar padded envelope, has been used
- It seems unusually heavy for its size. Most letters weigh up to about 28g or 1 ounce, whereas most effective letter bombs weigh 50-100g and are 5mm or more thick
- It has more than the appropriate value of stamps for its size and weight
- It is marked 'personal' or 'confidential'
- It is irregularly shaped or lopsided
- The envelope flap is stuck down completely (a harmless letter usually has an ungummed gap of 3-5mm at the corners)
- There is a pin-sized hole in the envelope or package wrapping
- There is a smell, particularly of almonds or marzipan
- There is an additional inner envelope, and it is tightly taped or tied (however, in some organisations sensitive or 'restricted' material is sent in double envelopes as standard procedure).

Chemical, biological or radiological materials in the post

Terrorists may seek to use chemical, biological or radiological materials in letter bombs. It is difficult to provide a full list of possible CBR indicators because of the diverse nature of the materials. However, some of the more common and obvious are:

- Unexpected granular, crystalline or finely powdered material (of any colour and usually with the consistency of coffee, sugar or baking powder), loose or in a container
- Unexpected sticky substances, sprays or vapours
- Unexpected pieces of metal or plastic, such as discs, rods, small sheets or spheres
- Strange smells, e.g. garlic, fish, fruit, mothballs, pepper, meat, marzipan. If you detect a smell, do not go on sniffing it. However, some CBR materials are odourless and tasteless
- Stains or dampness on the packaging
- Sudden onset of illness or irritation of skin, eyes or nose.

CBR devices containing finely ground powder or liquid may be hazardous without being opened.

What you can do:

- The precise nature of the incident (chemical, biological or radiological) may not be readily apparent. Keep your response plans general and wait for expert help from the emergency services
- Review plans for protecting staff in the event of a terrorist threat or attack. Remember that evacuation may not be the best solution. You will need to be guided by the emergency services on the day
- Plan for the shutdown of systems that may contribute to the movement of airborne hazards (e.g. computer equipment containing fans)
- Ensure that doors can be closed quickly if required
- If your external windows are not permanently sealed shut, develop plans for closing them in response to a warning or incident
- Examine the feasibility of emergency shutdown of air-handling systems and ensure that any such plans are well rehearsed
- Where a hazard can be isolated by leaving the immediate area, do so as quickly as possible, closing doors and windows as you go
- Move those directly affected by an incident to a safe location as close as possible to the scene of the incident, so as to minimise spread of contamination
- Separate those directly affected by an incident from those not involved so as to minimise the risk of inadvertent cross-contamination
- Ask people to remain in situ – though you cannot contain them against their will
- You do not need to make any special arrangements beyond normal first aid provision. The emergency services will take responsibility for treatment of casualties.

Planning your mail handling procedures

Although any suspect item should be taken seriously, remember that most will be false alarms, and a few may be hoaxes. Try to ensure that your procedures, while effective, are not needlessly disruptive. Take the following into account in your planning:

- Seek advice from your local police Counter Terrorism Security Advisor (CTSA) on the threat and on defensive measures
- Consider processing all incoming mail and deliveries at one point only. This should ideally be off-site or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the building
- Consider if possible, not receiving a normal mail delivery or unexpected packages on event day
- Ensure that all staff who handle mail are briefed and trained. Include reception staff and encourage regular correspondents to put their return address on each item
- Ensure that all sources of incoming mail (e.g. Royal Mail, couriers, and hand delivery) are included in your screening process
- Ideally post rooms should have independent air conditioning and alarm systems, as well as scanners and x-ray machines. However, while mail scanning may detect devices for spreading chemical, biological, and radiological (CBR) materials (and explosive devices), they will not detect the materials themselves
- At present, there are no CBR detectors capable of identifying all hazards reliably. Post rooms should also have their own washing and shower facilities, including soap and detergent
- Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual deliveries. Train them to open post with letter openers (and with minimum movement), to keep hands away from noses and mouths and always to wash their hands afterwards. Staff should not blow into envelopes or shake them. Packages suspected of containing biological, chemical or radiological material should ideally be placed in a double sealed bag
- Consider whether staff handling post need protective equipment such as latex gloves and facemasks (seek advice from a qualified health and safety expert). Keep overalls and footwear available in case they need to remove contaminated clothing
- Make certain post opening areas can be promptly evacuated. Rehearse evacuation procedures and routes, which should include washing facilities in which contaminated staff could be isolated and treated
- Staff responsible for mail handling should be made aware of the importance of isolation in reducing contamination
- Prepare signs for display to staff in the event of a suspected or actual attack.


WITHDRAWN 2017

nine search planning

Searches of stadia should be conducted as part of routine good housekeeping. They should also be conducted in response to a specific threat or when there is a general alert of attack.

As previously mentioned under Security Planning, it is ...gnised that for the majority of stadia responsibility for the implementation of any search p...g, following a vulnerability and risk assessment, will fall upon the Stadium S...Officer / Designated Person.

The following advice is generic for most stadia, bu...ognises that stadia are built and operate differently.

If considered necessary advice and gu...ching should be available from your local CTSA or Police Search Advisor (P...A).

Search Plans

- Search plans should be ...epar... in ...vance and staff should be trained in them.
- The conduct of s...che... will ...epend on local circumstances and local knowledge, but the overall objec...e is to ...ake sure that the entire premises and grounds are searched in a systemati... thorou... manner so that no part is left unchecked.
- If you ...cide to e...cuate your stadium in response to a threat, you will also need to search it in ...rde... ensure it is safe for re-occupancy.
- ...e po...e wi... not normally search stadia on every occasion it is used. (See High Profile ...ort... ...vents). They are not familiar with the layout and will not be aware of what ...ould be there and what is out of place. They cannot, therefore, search as quickly or as th...oughly as a member of staff or on site security personnel.
- The member(s) of staff nominated to carry out the search do not need to be expert 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.
- Ideally, searchers should search in pairs, to ensure searching is systematic and thorough.

Action You Should Take

Divide your stadium into sectors. If the stadium is organised into departments and sections, these should be identified as separate search sectors. Each sector must be of manageable size.

The sectorised search plan should have a written checklist - signed by a senior steward as completed for the information of the Stadium Safety Officer and Police Commander.

Remember to include stadium club shops, bars, vending outlets, stairs, corridors and lifts in the search plan, as well as car parks and other areas outside the building. If evacuation is considered or implemented, then a search of the evacuation point(s), the routes to them and the surrounding area should also be made.

Consider the most effective method of initiating the search. You could:

- Send a message to the search teams over a public address system (the messages should be coded to avoid unnecessary disruption and alarm)
- Use personal radios or pagers.

Ensure the searchers know what to do if they discover a suspicious item. Action will depend on the nature of the device and the location, but the general "golden rules" are:

- Do not touch the item or move it
- Move away from it immediately and keep spectators away
- Communicate what has been found to the Search Co-ordinator, using hand-held radios or mobiles only once out of the immediate vicinity and line of sight of the suspect item
- Remain on hand to brief the police on the exact location and its description.

The Stadium Safety Officer / Designated Person should liaise with the first police officers on the scene regarding safe evacuation distances.

Exercise your search plan regularly. The searchers need to get a feel for the logical progression through their designated area and the length of time this will take. They also need to be able to search without unduly alarming any spectators in the stadium.

Discuss your search plan with your local police Counter Terrorism Security Advisor (CTSA) or NaCTSA.

Searching of persons entering your stadium / arena

The security of your stadium relies on having some control over persons entering it. The security will differ on event days and non event days. As an event day approaches you may feel the need to increase the level of security at your stadium.

The best practice is to conduct a search and clear the area as previously described. This will give you confidence that your stadium is clear and fit for purpose. Having spent that time and effort searching your stadium the security could be compromised if you fail to take adequate steps to search persons entering the venue.

When the building search is complete all persons entering the stadium should go through a search regime. Dependent on the threat this search could be restricted to random bag searches or at times of a high security risk extend up to full body searches of every person entering the ground.

There is no statutory right of search by stewards; either within sports stadia or events arena. Searching as a condition of entry relies on the willingness of the individual to participate in that search and refusal to enter should they decline. This may often lead to conflict and requires to be managed carefully by stewards. Where submission to search by stewards is a condition of entry, this will not be carried out by police officers. (Police Constables within Scotland do have statutory powers of search in certain circumstances, particularly as it relates to designated sporting events, however officers may be required to satisfy a court that the circumstances are appropriate and justifiable). An example of best practice would be to ensure that police are aware of such condition of entry, which would allow for an accurate impact assessment to be made, which informs the most effective police response to the event.

Consider the following.

- Ensure that ground regulations include a right to refuse entry unless searched.
- Ensure that temporary staff have a clause within their contracts allowing them to be s ed.
- Consider advising spectators that searches will be carried out. They should rrive early and be encouraged not to bring bags. This can be achieved by mark of your website or pre-event advertising.
- Ensure you have properly briefed the searching staff on t and what they are searching for.
- Ensure the search areas have sufficient space.
- Consider separating queues into those with bag and who can be fast tracked through the search area.
- Ensure you have sufficient staff to y ou he sea ches.
- Search queues allow the profili of sp ators by security staff. This allows an opportunity to identify possible hostile onnai nce.
- Consider the fact that ectat s ofte arrive in large groups, close to the event start time. This can impact on the a ty o searchers to achieve their aims.
- Experience shows t when ere is a real threat from terrorism, most spectators not only accept sear ng, they tually expect to be searched. It instils confidence that an event is a safe envi nm t and an enjoyable experience.

See G od ractice C ecklist – Searching in Appendix 'D'

ten managing staff securely

Personnel Security

Some external threats, whether from criminals, terrorists, or competitors seeking a business advantage, may rely upon the co-operation of an 'insider'.

This could be an employee or any contract or agency staff (e.g. cleaner, caterer, steward, security guard) who has authorised access to your premises. If an employee, he or she may already be working for you, or may be someone newly joined who has infiltrated your organisation in order to seek information or exploit the access that the job might provide.

If you contract in staff who operate CCTV equipment, they must be licensed by the Security Industry Authority (SIA). This only applies if the CCTV equipment is deployed into fixed positions or has a pan, tilt and zoom capability and where operators:

- Proactively monitor the activities of members of the public whether they are in public areas or on private property
- Use cameras to focus on the activities of particular people either by directing or directing cameras to an individual's activities
- Use cameras to look out for particular individuals
- Use recorded CCTV images to identify individuals or to investigate their activities.

Since 20 March 2006, contract CCTV operators must carry an SIA CCTV (Public Space Surveillance) licence – it is illegal to work without one. Any security contractor should be aware of this and you should ensure that only licensed staff are supplied.

Much of the following advice simply falls under good recruitment and employment practice. During the recruitment process you should ask each candidate to:

- Confirm their full name, date of birth and address with a supporting official document such as a full current passport or British photo driving licence. Other useful identifying documents are P45, credit card with statements, birth certificate, cheque book and bank card with signature, bank statements (account documentation from any UK financial institution is particularly useful as they will usually have made their own checks before opening an account). Ask to see a recent utility bill(s) confirming the given address. **Do not accept** as proof of identity any duplicate or photocopied documents, an international driving licence, an old British visitor's passport or a birth certificate issued more than six weeks after birth
- Give their national insurance number or other government issued unique personal identifying number such as a National Health Insurance number
- Give evidence of academic or professional qualifications. Take up any references from schools, colleges, universities and previous employers (again, insist on originals) and check with the originators that they are genuine
- Give full details of previous employers (name, address and date) covering at least the past three years

- Give details of unspent convictions, where allowed under the Rehabilitation of Offenders Act 1974. In certain circumstances - for example, where the post involves working with children or vulnerable adults - employers who are registered with the Disclosure Scotland may seek details on the applicant's spent convictions. Remember, however, that a conviction - spent or unspent - need not be a bar to employment
- To provide proof of the right to work in the UK if relevant. For European Economic Area (EEA) nationals, ask to see their national identity card or passport and Home Office documentation confirming immigration status and permission to work.

Having obtained this information, check it: the increasing availability of personal good quality false documentation on the Internet has made establishing identity more a problem than it used to be. Also look out for any obvious gaps and inconsistencies in the applicant's employment or residential history.

All this will take time, so if you need the candidate to start work quickly or an offer of employment is made, then make the satisfactory completion of checks a condition of employment. In all cases, remind applicants that supplying false information, or failing to disclose relevant information, could be grounds for dismissal and could amount to a criminal offence.

Personnel procedures intended to prevent criminal activity or terrorism may be regarded as unwelcome and intrusive. Whatever the circumstances, measures should be demonstrably proportionate to the perceived risk and as fair as possible; staff should understand the risks and accept the measures taken to mitigate them.

Think along the following lines:

- Make it easy for staff to discuss their concerns confidentially and informally
- Encourage managers and staff to be alert to anything unusual in employees' behaviour or attitudes, reassuring them that any information will be handled sensitively and confidentially. Note that any action taken as a result of such concerns must be in accordance with employment law
- Operate a security awareness programme to remind managers and staff of potential threats, both internal and external, and of their roles in countering them
- Permit access to sensitive locations, assets or information only to those who genuinely need it
- Consider imposing physical controls to restrict access to particularly sensitive areas, or random searching on entry and exit of staff in such areas. Explain the reasons behind such intrusive action.

After recruitment it is important that staff are monitored and supervised to identify any changing or suspicious behaviour that might suggest unreliability or conflict of interest. Ongoing personnel security is best achieved by creating a culture in which security is important and accepted. It should be easy for staff and managers to discuss their concerns and problems confidentially and informally and to voice any concerns they may have about others.

You may want to consider some form of confidential reporting line, sometimes known as whistle blowing.

Staff might be affected by altered circumstances that compromise their trustworthiness regardless of their professional standing and previous reliability. This can be the result of a wide range of life events, from stressful personal or working circumstances to deliberate recruitment by malicious third parties.

Circumstances leading to vulnerability might be subtle and difficult to recognise but could include financial difficulty, peer, family or external group pressure and perceptions of unfairness at work.

Other potential warning signs to watch out for are:

- Drug or alcohol misuse
- Expression of support for violence-prone views, actions or incidents
- Major unexplained changes in lifestyle or expenditure
- Sudden loss of interest in work, or overreaction to career chang intments
- Manifestations of stress such as over-emotional behaviour
- Unusual interest in security measures or areas of work o normal remit
- Changes in working patterns, for instance working a t unusual hours, failing to take holidays
- Frequent unexplained absences
- Repeated failure to follow recognised dure
- Unusual travel abroad
- Relationships with or suppo divi ls or institutions that are generally regarded as professionally suspect
- Sudden or marked ch e in ligi s, political or social affiliation or practice which has an adverse impa t on t divi al's performance or attitude to security.

Individual ca will have ique features and it may take a combination of behaviours and attitudes to war t further concern. It is important to note that some of these signs may be the re ult of ill-heal . You should allow for this in your consideration of them.

You m also ish to consider whether to undertake checks for existing staff where this has not alre been done to a satisfactory level.

If you have serious reason to suspect that you are being bugged or subject to other forms of ele nic eavesdropping, do not report your suspicions over a telephone or from the place that is suspect. Use a public telephone box or mobile phone away from the building in question.

There are some commercial security firms that can sweep your premises and equipment, but report any serious suspicions of espionage on behalf of terrorists or foreign powers to the police.

Contractors and agency staff

The use of contractors and agency staff for an increasing range of services (e.g. IT support, cleaning, catering, security guarding, stewarding of events and consultancy) can create additional vulnerabilities and expose organisations to greater personnel security risks. While some agencies may be careful in their selection procedures, the less rigorous are open to exploitation by terrorists and sympathisers. Therefore, you should:

- Make it a contractual obligation that contractors validate the identities and bona fides of their staff
- Conduct regular monitoring of your contractor's compliance with the contract
- Establish that the contractor is part of a recognised professional organisation responsible for accrediting standards in that industry
- Confirm that the individual sent by the contractor or agency is the person who actually turns up. For instance, ask the contractor to provide an authenticated photo of the individual, together with their full name, in advance of arrival. Ask the individual to provide photo ID that can be checked on entry
- Provide passes (with a photo) to contract staff, once you are satisfied that the person who turns up on the day is genuine. The pass must be worn at all times. Ideally, the employer should retain the pass between visits and hand it over only once the photo has been checked
- Agree a procedure for substituting contract staff with temporary replacements when the usual contract staff are away or consider whether the replacement's duties or access need to be restricted
- Supervise where possible contract staff whenever they are on the premises and particularly if they have access to sensitive areas
- Consider additional registration of stewards on the National Stewards Database under the control of the football authorities and based at the Football League
- Nominate a permanent member of staff to be responsible in personnel terms for contract staff (i.e. not merely for overseeing delivery of the contract), so that potential problems, such as conflicts of loyalty, may be identified and addressed early.

See Good Practice Checklist – Managing Staff Securely in Appendix 'E'.

eleven information security

The theft, copying or destruction of information is a growing problem for many organisations. Your confidential information may be of interest to business competitors, criminals, foreign intelligence services or terrorists. They may attempt to access your information by breaking into your IT systems, by obtaining the data you have thrown away or by infiltrating your organisation. Such an attack could disrupt your business and damage your reputation.

Before taking specific protective measures you should:

- Assess the threat and your vulnerabilities. To what extent is your information at risk, who might want it, how might they get it, how would its loss or theft damage you?
- Consider basic security measures to protect paper-based information such as operating a clear desk policy, not leaving sensitive information lying around or displayed on notice boards, using secure cabinets, locking appropriate doors and providing guidance to staff, especially those who have to take information off the premises.

Cyber attack

A *Cyber attack could:*

- Allow the attacker to remove sensitive information
- Allow the attacker to gain access to your computer system and do whatever the system owner can do. This could include modifying your data, perhaps subtly so that it is not immediately apparent, or installing hardware or software devices to relay information back to the attacker. Such attacks against Internet-connected systems are extremely common.
- Make your systems impossible to use through 'denial of service' attacks. These are increasingly common, relatively simple to launch and difficult to protect against.

As soon as you entrust your information or business processes to a computer system, they are at risk. Cyber attacks are much easier when computer systems are connected directly or indirectly to public networks such as the internet.

The typical methods of cyber attack are:

Hacking

This is an attempt at unauthorised access, almost always with malicious or criminal intent. Sophisticated, well-concealed attacks by foreign intelligence services seeking information have been aimed at government systems but other organisations might also be targets.

Malicious software

The techniques and effects of malicious software (e.g. viruses, worms, trojans) are as variable as they are widely known. The use of e-mail, systems that interconnect, external contractors and remote access (e.g. for home working) allows virus infections to spread ever more widely and rapidly.

Malicious modification of hardware

Computer hardware can be modified so as to mount or permit a cyber attack. This is normally done at the point of manufacture or supply prior to installation, though it could also be done during maintenance visits. The purpose of such modifications would be to allow a subsequent attack to be made, possibly by remote activation.

Denial of service (DoS)

These attacks aim to overwhelm a system by flooding it with unwanted data. Some DoS attacks are distributed, in which large numbers of unsecured, 'innocent' machines (known as 'zombies') are conscripted to mount attacks.

As with other security measures, you should conduct a risk assessment to establish whether you might be at particular risk from a cyber attack. System security professionals can provide detailed advice.

What to do

- Acquire your IT systems from reputable manufacturers and suppliers
- Ensure that your software is regularly updated. Suppliers are continually fixing security vulnerabilities in their software. These fixes or patches are available from their websites – consider checking for patches and updates at least weekly
- Ensure that all internet-connected computers are equipped with anti-virus software and are protected by a firewall
- Back up your information, preferably keeping a secure copy in another location
- Assess the reliability of those who maintain, operate and guard your systems (refer to the section on Managing staff securely on page 29)
- Consider encryption packages for material you want to protect, particularly if taken off-site – but seek expert advice first
- Take basic security precautions to prevent software or other sensitive information falling into the wrong hands. Encourage security awareness among your staff, training them not to leave sensitive material lying around and to operate a clear desk policy (i.e. desks to be cleared of all work material at the end of each working session)
- Make sure your staff are aware that users can be tricked into revealing information which can be used to gain access to a system, such as user names and passwords
- Invest in secure cabinets, fit locking doors and ensure the proper destruction of sensitive material
- Where possible, lock down or disable disk drives, USB ports and wireless connections
- Ensure computer access is protected by securely controlled, individual passwords or by biometrics and passwords.

Organisations can seek advice from the Government website - www.getsafeonline.org and www.cpni.gov.uk.

Examples of cyber attacks

- A former systems administrator was able to intercept e-mail between company directors because the outsourced security services supplier had failed to secure the system
- A former employee was able to connect to a system remotely and made changes to a specialist digital magazine, causing loss of confidence among customers and shareholders.

Disposal of sensitive information

Companies and individuals sometimes need to dispose of sensitive information. Some of the material that businesses routinely throw away could be of use to a wide variety of groups including business competitors, identity thieves, criminals and terrorists.

The types of information vary from staff names and addresses, telephone numbers, product information, customer details, information falling under the Data Protection Act, technical specifications and chemical and biological data. Terrorist groups are known to have shown interest in the last two areas.

The principal means of destroying sensitive waste are:

Shredding

A cross-cutting shredder should be used so that no two adjacent characters are legible. This produces a shred size of 15mm x 4mm assuming a text font size of 12.

Incineration

Incineration is probably the most effective way of destroying sensitive waste, including disks and other forms of magnetic and optical media, provided a suitable incinerator is used (check with your local authority).

Open fires are not reliable as material is not always destroyed and legible papers can be distributed by the updraft.

Pulping

This reduces waste to a fibrous state and is effective for paper and card waste only. However, some pulping machines merely tear the paper into large pieces and turn it into a papier maché product from which it is still possible to retrieve information. This is more of a risk than it used to be because inks used by modern laser printers and photocopiers do not run when wet. There are alternative methods for erasing digital media, such as overwriting and degaussing. For further information visit www.cpni.gov.uk

Before investing in waste destruction equipment you should:

- If you use contractors, ensure that their equipment and procedures are up to standard. Find out who oversees the process, what kind of equipment they have and whether the collection vehicles are double-manned, so that one operator remains with the vehicle while the other collects. Communications between vehicle and base are also desirable
- Ensure that the equipment is up to the job. This depends on the material you wish to destroy, the quantities involved and how confidential it is
- Ensure that your procedures and staff are secure. There is little point investing in expensive equipment if the people employed to use it are themselves a security risks
- Make the destruction of sensitive waste the responsibility of your security department rather than facilities management.

See good practice checklist – Information Security in Appendix 'F'

twelve vehicle borne improvised explosive devices (VBIEDs)

Vehicle Borne Improvised Explosive Devices (VBIEDs) are one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives to a target and can cause a great deal of damage.

Once assembled, the bomb can be delivered at a time of the terrorist's choosing and with reasonable precision, depending on defences. It can be detonated from a safe distance using a timer or remote control, or can be detonated on the spot by a suicide bomber.

Building a VBIED requires a significant investment of time, resources and expertise. Because of this, terrorists will seek to obtain the maximum impact for their investment. They generally choose high-profile targets where they can cause the most damage, inflict mass casualties or attract widespread publicity.

Effects of VBIED's

VBIED's can be highly destructive. It is not just the effects of a direct hit or blast that can be lethal, flying debris such as glass can present a hazard many metres away from the point of a VBIED.

What you can do

If you think your stadium could be at risk from any form of VBIED you should:

- Ensure basic good housekeeping such as vehicle access controls and parking restrictions. Do not allow unchecked vehicles to park next to or under your stadium
- Consider using physical barriers to keep away unauthorised vehicles at a safe distance. Seek the advice of your local police Counter Terrorism Security Advisor (CTSA) on what these should be and on further measures such as electronic surveillance including Automatic Number Plate Recognition (ANPR) and protection from flying glass
- Insist that vehicles permitted to approach your stadium are authorised in advance, searched, and accompanied throughout. The identity of the driver should be cleared in advance. **It may be necessary to carry out a risk assessment for the assistance of security staff who may be involved in vehicle access control**
- Do what you can to make your stadium blast resistant, paying particular attention to windows. Have the stadium reviewed by a qualified security engineer when seeking advice on protected spaces, communications, announcement systems and protected areas
- Exhibit and rehearse bomb threat and evacuation drills. Bear in mind that, depending on where the suspected VBIED is parked and the design of your building, it may be safer in windowless corridors or basements than outside
- Assembly areas must take account of the proximity to the potential threat. You should bear in mind that a vehicle bomb delivered into your building – for instance via underground car parks or through the front of your premises – could have a far greater destructive effect on the structure than an externally detonated device
- Train and exercise your staff in identifying suspect vehicles, and in receiving and acting upon bomb warnings. Key information and telephone numbers should be prominently displayed and readily available.

It should be emphasised that the installation of physical barriers needs to be balanced against the requirements of safety and should not be embarked upon without full consideration of planning, fire and other stadium regulation.

See Good Practice Checklist – Access Control in Appendix 'B'

thirteen chemical, biological and radiological (CBR) attacks

Since the early 1990s, concern that terrorists might use CBR materials as weapons has steadily increased. The hazards are:

Chemical

Poisoning or injury caused by chemical substances, including ex-military chemical warfare agents or legitimate but harmful household or industrial chemicals.

Biological

Illnesses caused by the deliberate release of dangerous bacteria, viruses or fungi, or biological toxins such as the plant toxin ricin.

Radiological

Illnesses caused by exposure to harmful radioactive material contaminating the environment.

A radiological dispersal device (RDD), often referred to as a 'dirty bomb', is typically a device where radioactive materials are combined with conventional explosives. Upon detonation, no nuclear explosion is produced but, depending on the type of the radioactive source, the surrounding areas become contaminated.

As well as causing a number of casualties from the initial blast, there may well be a longer-term threat to health. A number of terrorist groups have expressed interest in, or attempted to use, a 'dirty bomb' as a method of attack.

Much of the CBR-related activity seen to date has either been criminal, or has involved hoaxes and false alarms. There have only been a few examples of terrorists using CBR materials. The most notable were the 1995 sarin gas attack on the Tokyo subway, which killed twelve people, and the 2001 anthrax letters in the United States, which killed five people.

CBR weapons have been little used so far, largely due to the difficulty of obtaining the materials and the complexity of using them effectively. Where terrorists have tried to carry out CBR attacks, they have generally used relatively simple materials. However, Al Qaida and related groups have expressed a serious interest in using CBR materials. The impact of any terrorist CBR attack would depend heavily on the success of the chosen dissemination method and the weather conditions at the time of the attack.

The likelihood of a CBR attack remains low. As with other terrorist attacks, you may not receive prior warning of a CBR incident. Moreover, the exact nature of an incident may not be immediately obvious. First indicators may be the sudden appearance of powders, liquids or strange smells within the building, with or without an immediate effect on people.

Good general physical and personnel security measures will contribute towards resilience against CBR incidents. Remember to apply appropriate personnel security standards to contractors, especially those with frequent access to your site.

What you can do.

- Review the physical security of your air-handling systems, such as access to intakes and outlets
- Improve air filters or upgrade your air-handling systems, as necessary
- Restrict access to water tanks and other key utilities
- Review the security of your food and drink supply chains
- Consider whether you need to make special arrangements for mail or parcels (e.g. a separate post room, possibly with dedicated air-handling, or even a specialist off-site facility. (See Mail Handling)
- The Home Office advises organisations against the use of CBR detection technologies as part of their contingency planning measures at present. This is because the technology is not yet proven in civil settings and, in the event of a CBR incident, the emergency services would come on scene with appropriate detectors and advise accordingly. A basic awareness of CBR threat and hazards, combined with general protective security measures (e.g. screening visitors, CCTV monitoring of perimeter and entrance areas, being alert to suspicious letters and packages) should offer a good level of resilience. In the first instance, seek advice from your local CTSA
- If you have a designated protected space that may also be suitable as a CBR shelter, but seek specialist advice from your local police CTSA before you make plans to use it in this way
- Consider how to communicate necessary safety advice to staff and how to offer reassurance. This needs to include instructions to those who want to leave, return to or enter the building.

fourteen suicide attacks

Suicide bombers may use a lorry, plane or other kind of vehicle as a bomb or may conceal explosives on their person. Both kinds of attack are generally perpetrated without warning. The most likely targets are symbolic locations, key installations, VIPs or mass-casualty crowded places and 'soft' targets.

When considering protective measures against suicide bombers, think in terms of:

- Denying access to any vehicle or anything that has not been thoroughly searched. Ensure that no one visits your protected area without your being sure of his or her identity or without proper authority. Seek further advice through your local police CTSA
- Establishing your search area at a distance from the protected site, setting up regular patrols and briefing staff to look out for anyone behaving suspiciously; many bomb attacks are preceded by reconnaissance or trial runs. Ensure that any suspicious behaviour is reported to the police
- Effective CCTV systems can help prevent or even deter hostile reconnaissance, and can provide crucial evidence in court
- There is no definitive physical profile for a suicide bomber, so remain vigilant and report anyone suspicious to the police.

See Hostile Reconnaissance - page 45

fifteen firearm and weapon attacks

Terrorist use of firearms and weapons is still infrequent, but it is important to consider this method of attack and be prepared to cope with such an incident. Below is some general guidance to aid your planning in this area.

Stay Safe

- Find the best available ballistic protection.
- Remember, out of sight does not necessarily mean out of danger, especially if y[illegible] not ballistically protected.

GOOD COVER	BAD COVER
Substantial Brickwork or Concrete	Internal Partition W[illegible]
Engine Blocks	Car Doors
Base of Large Live Trees	Wooden Fenc[illegible]
Natural Ground Undulations	Glazin[illegible]

See

- It is a firearms / weapons incident.
- Exact location of the incident.
- Number of gunmen.
- Type of firearm - are they using [illegible] barrelled weapon or handgun
- Direction of travel - are they mo[illegible]g [illegible]any particular direction

Consider the use of CCT[illegible] and other r[illegible]ote methods of confirmation reducing vulnerabilities to staff.

Tell

- **Who** - Im[illegible]diately c[illegible]ntact the police by calling 999 or via your control room, giving them the in[illegible]matio[illegible]sho[illegible]n under **Confirm**
- **How** - [illegible]ll the channels of communication available to you to inform visitors and staff of th[illegible]nger.
- **Plan** [illegible]or a firearms / weapons incident.
    1. How you would communicate with staff and visitors
    2. What key messages would you give to them in order to keep them safe.
    3. Think about incorporating this into your emergency planning and briefings
- **Test** - your plan before you run your event

Act

- As far as you can, limit access and secure your immediate environment.
- Encourage people to avoid public areas or access points. If your have rooms at your location, lock the doors if possible and remain quiet.

See Physical Security on page 11.

If you require further information please liaise with your Counter Terrorism Security Advisor (CTSA) .

sixteen communication

You should consider a communication strategy for raising awareness among staff and others who need to know about your security plan and its operation. This will include the emergency services, local authorities and possibly neighbouring premises.

There should also be arrangements for dealing with people who may be affected by your security operation but who are not employees of your organisation (e.g. customers, clients, contractors, visitors).

Security issues should be discussed / decided at Board level and form a part of the organisation's culture.

Stadium Safety Officers / Designated Persons should regularly meet with staff to discuss security issues and encourage staff to raise their concerns about security.

Consideration should be given to the use of the organisation's website, programme, publications and tickets to communicate crime prevention and counter terrorism initiatives.

All Stadia should have a supply of posters and material (even via web links) to support crime prevention and counter terrorism messages and initiatives.

All Stadium Safety Officers / Designated Persons should involve their local police Counter Terrorism Security Adviser when considering improvements to the stadium and / or its environs.

See Good Practice Checklist – Communication in Appendix 'G'

seventeen hostile reconnaissance

Operation Lightning is a national intelligence gathering operation to record, research, investigate and analyse:

- Suspicious sightings
- Suspicious activity

at or near:

- Crowded places

or prominent or vulnerable:

- Buildings
- Structures
- Transport infrastructure.

The ability to recognise those engaged in hostile reconnaissance might disrupt an attack and produce important intelligence leads.

Primary Role of Reconnaissance

- Obtain a profile of the target location
- Determine the best method of attack
- Determine the optimum time to conduct the operation.

Hostile reconnaissance is used to provide information to operational planners on potential targets during the preparatory and operational phases of terrorist operations.

Where pro-active security measures are in place, particular attention is paid to monitor any variations in security patterns and the flow of people in and out.

What to look for.

- Significant interest being taken in the outside of the Stadium / Arena including parking areas – delivery gates – doors – entrances
- Groups or individuals taking significant interest in the location of CCTV cameras and controlled areas
- People taking pictures – filming – making notes – sketching of the security measures at Stadia / Arena. Tourists should not necessarily be taken as such and should be treated sensitively, but with caution
- Overt / covert photography, video cameras, possession of photographs, maps, blueprints etc, of critical infrastructures, electricity transformers, gas pipelines, telephone cables etc
- Possession of maps, global positioning systems (GPS), photographic equipment, (cameras, zoom lenses, camcorders). GPS can assist in the positioning and correct guidance of

weapons such as mortars and Rocket Propelled Grenades (RPGs). This should be considered a possibility up to 1000 yards from any target

- Attempts to disguise identity – motorcycle helmets, hoodies etc, or multiple sets of clothing to change appearance
- Vehicles Parked outside buildings of other facilities, with one or more people remaining in the vehicle, for longer than would be considered usual
- Parking, standing or loitering in the same area on numerous occasions with no apparent reasonable explanation
- Prolonged static surveillance using operatives disguised as demonstrators, street sweepers, etc or stopping and pretending to have car trouble to test response times for emergency services, car recovery companies, (AA, RAC etc) or local staff
- Simple observation such as staring or quickly looking away
- Activity inconsistent with the nature of the building
- Noted pattern or series of false alarms indicating possible testing of security systems and observation of response behaviour and procedures, (bomb threats, leaving hoax devices or packages)
- The same vehicle and different individuals or changed individuals in a different vehicle returning to a location(s)
- The same or similar individuals returning to carry out the same activity to establish the optimum time to conduct the operation
- Unusual activity by contractor's vehicles
- Recent damage to perimeter security, breaches in fence lines or walls or the concealment in hides of mortar base plates or assault equipment, i.e. ropes, ladders, food etc. Regular perimeter patrols should be instigated months in advance of an event to ensure this is not happening
- The same individual changing multiple sets of clothing to give the appearance of being a different individual

Constant use of different paths – access routes – across a site. 'Learning the route' or foot surveillance involving a number of people who seem individual but are working together

- Multiple identification documents – suspicious, counterfeit, altered documents etc

Non co-operation with police or security personnel

- Those engaged in reconnaissance will often attempt to enter premises to assess the internal layout and in doing so will alter their appearance and provide cover stories
- In the past reconnaissance operatives have drawn attention to themselves by asking peculiar & in depth questions of employees or others more familiar with the environment

Reconnaissance operatives will seek information on:

- Width surveys of surrounding streets – exploring the range of tactical options available to deliver the device
- Levels of internal and external security – are person / bag searches undertaken.

THE ROLE OF THE RECONNAISSANCE TEAM HAS BECOME INCREASINGLY IMPORTANT TO TERRORIST OPERATIONS.

Reconnaissance trips may be undertaken as a rehearsal to involve personnel and equipment that will be used in the actual attack e.g. before the London attacks on 7th July 2005, the bombers staged a trial run nine days before the actual attack.

Reporting suspicious activity to police that does not require an immediate response, contact the ANTI-TERRORIST HOTLINE – 0800 789 321

ANY INCIDENT THAT REQUIRES AN IMMEDIATE RESPONSE – DIAL 999.


WITHDRAWN 2017

eighteen high profile events

Some events will, for various reasons, be deemed to be more high profile than events that normally take place at your stadium / arena.

In certain cases the Police Gold Commander with responsibility for the event may appoint a Security Co-ordinator (SecCo) and / or a Police Search Advisor (PoISA).

Security co-ordinator - SecCo

The Security Co-ordinator (SecCo) has a unique role in the planning and orchestration of security measures at high profile sporting events.

The SecCo works towards the strategy set by the Police Gold Commander and acts as an adviser and co-ordinator on security issues.

A number of options and resources are available to the SecCo, which will include identifying all the key individuals, agencies and departments involved in the event as well as seeking advice from the relevant CTSA.

The SecCo will provide the Gold Commander with a series of observations and recommendations to ensure that the security response is realistic and proportionate.

Within Scotland Police Command and Control structure and role, follows Strategic, Tactical and Operational Command as opposed to Gold, Silver and Bronze Command.

Police search advisor - PoISA

The SecCo can deem it necessary to appoint a Police Search Advisor (PoISA) to a high profile sporting event.

The PoISA will carry out an assessment of the venue and nature of the event, taking into consideration an up to date threat assessment and other security issues.

A report, including the PoISA assessment, recommendations and subsequent search plan will be submitted through the SecCo to the Gold Commander.

good practice checklists

The following checklists are intended as a guide for stadium and arena management to assist them in identifying the hazards and risks associated with stadium counter terrorism planning.

They are not however exhaustive and some of the guidance might not be relevant to all stadia and arenas.

The checklists should be considered taking the following factors into account:

- What is relevant to your stadium or arena?
- Have you consulted your police CTSA?
- Who else should be included during consultation?
- Which measures can be implemented with ease?
- Which measures will take greater planning and investment?

appendix a

Housekeeping Good Practice

	Yes	No	Unsure
Have you reviewed the use and location of all waste receptacles in and around your stadium / arena?			
Do you keep external areas, entrances, exits, foyers, reception areas and toilets clean and tidy?			
Do you keep furniture to a minimum to provide little opportunity to hide devices?			
Are unused offices, rooms and function suites locked?			
Do you use seals/locks to secure maintenance hatches, compactors and industrial waste bins when not required for immediate use?			
Do you have an agreed protocol in place for the security of outside broadcast vehicles, equipment and personnel?			
Do you screen all your mail and do you cancel all normal mail and parcel deliveries on event days?			
Are your reception staff and deputies trained and competent in handling telephoned bomb threats?			
Have you considered marking your first aid fire fighting equipment as stadium property and checking that it has not been replaced immediately prior to an event?			

appendix b

Access Control and Visitors to Stadiums / Arenas

	Yes	No	Unsure
Is there clear demarcation identifying the public and private areas of your stadium / arena? (Not public entrances or turnstiles on event days).			
Do you prevent vehicles from parking close to the stadium / arena or under the structure?			
Do you have access control measures for persons and vehicles (including vehicle I.D. passes) on both event and non event days?			
Do your staff wear ID badges at all times when in the stadium / arena?			
Do you adopt a 'challenge culture' to anybody not wearing a pass?			
Are all stewards, caterers and other employees issued w photographic and barcode identification retained on date database and checked before access is permitted			
Are Senior Police, Ambulance, Fire Brigade and Managers asked to supply the Stadium Safety O er / Designated Person with details of staff and hat wi be attending the event?			
Are Safety Officers / Designated Per wards informed in advance of delivery, waste collection or's vehicle and driver's details?			
Do you have an access trol licy for ccredited press and photographers, allowing those whose identity is confirmed and ha advance?			
Do you ask ide broa ast companies to provide in advance to the Stadium S y Office Designated Person details of staff and vehi that be tending the event?			
Do ll visit e to report to a reception area before entry?			
o yo cilitate the arrival of VIPs, players and officials and appoint wards to assist them?			
non event day visitors asked for proof of ID and issued with visi badges?			
Are all visitors asked to sign in when they enter the building?			
Are visitors' badges designed to look different from staff badges?			
Are all visitors' badges collected from visitors when they leave the building?			
Does a member of staff accompany visitors at all times while in the building?			
During stadium tours do the tour guides have complete control and supervision of the visitors at all times in all areas?			
Are details of all people using community facilities within the stadium provided to Safety Officers / Designated Persons / Stewards?			

appendix C

CCTV

	Yes	No	Unsure
Do you constantly monitor your CCTV images or playback overnight recordings for evidence of suspicious activity?			
Do you have your CCTV cameras regularly maintained?			
Do the CCTV cameras cover the entrances and exits to your building?			
Do you have CCTV cameras covering critical areas in your business, such as server rooms, back up generators or cash offices?			
Do you store the CCTV images in accordance with the evidential needs of the police?			
Could you positively identify an individual from the recorded images on your CCTV system?			
Are the date and time stamps of the system accurate?			
Does the lighting system compliment the CCTV system during daytime and darkness hours?			
Do you regularly check the quality of your recordings?			
Are your 'contracted in' CCTV operators licensed in accordance with Security Industry Authority (SIA) guidelines?			
Have you implemented operating procedures, codes of practice and audit trails?			
Is each CCTV camera doing what it was installed to?			

appendix d

Searching

	Yes	No	Unsure
Do you operate an overt bag searching regime outside the stadium to act as a visual deterrent?			
Do you operate random searches of spectators in order to demonstrate a robust regime?			
Do you conduct random overt searches of vehicles as a visual deterrent?			
Do you carry out selective random searching of staff – again as an overt visual deterrent?			
Have you in place a policy for searching contractors, stewards, caterers, local franchises and restrict their ability to enter the stadium with baggage?			
Do you deny access to anyone or any thing that has not been thoroughly searched?			
Do you have a sectorised search plan with written checklist – signed by a senior steward as completed for the confirmation of the Stadium Safety Officer and Police Commander?			
Do all stadium bars, restaurants and kiosks that open after commencement of the event have a search procedure with sign-off checklist so that suspect packages are not overlooked?			
Do you regularly search vendor's equipment around the stadium as crowds gather before the event and prior to dispersal?			
Do you search all executive boxes prior to an event and log the result for the Safety Officer?			
Have you considered training stewards in profiling people as they approach the search regime?			
Do you make use of your website / programme / tickets to inform spectators in advance of searching policies as well as crime prevention and counter terrorism messages?			
Do your regulations include a right to refuse entry unless searched?			
Are your searching staff properly briefed on their powers and what they are searching for?			
If you are not body searching, can you fast track spectators with no baggage?			
Do you have a sufficient number of searchers and space to search effectively?			
Will you be able to cope with a large number of spectators arriving just before the event starts?			

appendix e

Managing Staff Securely

	Yes	No	Unsure
During recruitment do you require:			
Full name?			
Current address and any previous addresses in last five years?			
Date of birth?			
National Insurance number?			
Full details of references (names, addresses and contact details)?			
Full details of previous employers, including dates of employment?			
Proof of relevant educational and professional qualifications?			
Proof of permission to work in the UK for non-British or non-European Economic Area (EEA) nationals?			
Do you ask British citizens for:			
Full (current) 10-year passport?			
British driving licence (ideally the photo licence)?			
P45?			
Birth Certificate – issued within six weeks of birth?			
Credit card – with three statements and proof of signa			
Bank card – with three statements and p of gnatur			
Proof of residence – council tax, q ctric ater or telephone bill?			
EEA Nationals:			
Full EEA passport			
National Identity Ca			
Other Natio s:			
Full Passp t an			
A Hom ffice docu nt confirming the individual's UK Imm ati tus and permission to work in UK?			
the ewar employed by the organisation registered on the atio wards database?			

appendix f

Information Security

	Yes	No	Unsure
Do you lock away all business documents at the close of the business day?			
Do you have a clear-desk policy out of business hours?			
Do you close down all computers at the close of the business day?			
Are all your computers password protected?			
Do you have computer firewall and antivirus software on your computer systems?			
Do you regularly update this protection?			
Have you considered an encryption package for sensitive information you wish to protect?			
Do you destroy sensitive data properly when no long[illegible] req[illegible]ed?			
Do you back up business critical information reg[illegible]larly?			
Do you have a securely contained back up at a [illegible]tion from where you operate your business? ([illegible]back [illegible]oced[illegible])			
Have you invested in secure cabinets for your IT [illegible]ment?			

appendix g

Communication

	Yes	No	Unsure
Are security issues discussed / decided at Board level and form a part of your organisation's culture?			
Do you have a security policy or other documentation showing how security procedures should operate within your business?			
Is this documentation regularly reviewed and if necessary updated?			
Do you regularly meet with staff and discuss security issues?			
Do you encourage staff to raise their concerns about security?			
Do you know your local Counter Terrorism Security Advisor (CTSA) and do you involve him/her in any stadium or security developments?			
Do you speak with neighbouring businesses on issues of security and crime that might affect you all?			
Do you remind your staff to be vigilant when travelling to and from work, and to report anything suspicious to the relevant authorities or police?			
Do you make use of your website, programme or tickets to communicate crime and counter terrorism initiatives, including an advance warning re searching?			

What do the results show?

Having completed the various 'Good Practice' checklists you need to give further attention to the questions that you have answered 'no' or 'don't know' to.

If you answered 'don't know' to a question, find out more about that particular issue to reassure yourself that your vulnerability is being addressed or needs to be addressed.

If you answered 'no' to any question then you should seek to address that particular issue as soon as possible.

Where you have answered 'yes' to a question, remember to regularly review your security measures to make sure that your security measures are fit for that purpose.

bomb threat checklist

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

Visit www.mi5.gov.uk to download a PDF and print it out.

Actions to be taken on receipt of a bomb threat:

- Switch on tape recorder (if connected)

- Record the exact wording of the threat:

_____

_____

Ask the following questions:

- where is the bomb right now? _____

- when is it going to explode? _____

- what does it look like? _____

- what kind of bomb is it? _____

- what will cause it to explode? _____

- did you place the bomb? _____

- why? _____

- what is your name? _____

- what is your address? _____

- what is your telephone number? _____

Record time call completed: _____

Where automatic number reveal equipment is available, record number shown:

_____

Inform the Safety Officer - Name and telephone number of the person informed:

_____

Contact the police on 999. Time informed: _____

The following part should be completed once the caller has hung up and the Safety Officer (or, if the Safety Officer is not available, the police) has been informed.

Time and date of call: _____

Length of call: _____

Number at which call was received (i.e. your extension number): _____

ABOUT THE CALLER

Sex of caller: _____

Nationality: _____

Age: _____

THREAT LANGUAGE (tick)

❒ Well spoken?

❒ Irrational?

❒ Taped message?

❒ Offensive?

❒ Incoherent?

❒ Message read by threat-maker?

CALLER'S VOICE (tick)

❒ Calm?

❒ Crying?

❒ Clearing throat?

❒ Angry?

❒ Nasal?

❒ Slurred?

❒ Excited?

❒ Stutter?

❒ Disguised?

❒ Slow?

❒ Lisp?

❒ Ac nt? If so, what type?_____

❒ pid

❒ eep?

❒ se?

❒ Laughter?

❒ Familiar? If so, whose voice did it sound like? _____

BACKGROUND SOUNDS (tick)

❒ Street noises?

❒ House noises?

❒ Animal noises?

❒ Crockery?

❒ Motor?

❒ Clear?

❒ Voice?

❒ Static?

❒ PA stem

❒ Booth?

❒ Mu

❒ tory machinery?

❒ Office machinery?

❒ Other? (specify) _____

OTHER REMARKS

_____

_____

_____

_____

Signature

_____

Date _____

Print name

_____

useful publications and contacts

Publications

Protecting Against Terrorism (3rd Edition)
This publication provides general protective security advice from the Centre for the Protection of National Infrastructure CPNI. It is aimed at businesses and other organisations seeking to reduce the risk of a terrorist attack, or to limit the damage terrorism might cause. The booklet is available in PDF format and can be downloaded from www.cpni.gov

Expecting the Unexpected
This guide is the result of a partnership between the business community, police and business continuity experts. It advises on business continuity in the event and aftermath of an emergency and contains useful ideas on key business continuity management processes and a checklist.

Secure in the Knowledge
This guide is aimed mainly at small and medium-size businesses. It provides guidance and information to help improve basic security. Ideally it should be read in conjunction with Expecting the Unexpected which is mentioned above. By following the guidance in both booklets, companies are in the best position to protect, manage and recover from a range of threats to their business.

Both booklets are available to download at www.nactso.gov.uk and www.gov.uk

Contacts

National Counter Terrorism Security Office
www.nactso.gov.uk

MI5 - Security Service
www.mi5.gov.uk

Home Office
www.gov.uk

Department of Culture, Media & Sport
www.gov.uk

Association of Chief Police Officers
www.acpo.police.uk

Centre for Applied Science and Technology
www.gov.uk

Information Security
www.getsafeonline.org

Centre for the Protection of the National Infrastructure
www.cpni.gov.uk

Football Licensing Authority
www.flaweb.org.uk/fla

The Football League
www.football-league.co.uk

Football Safety Officers Association
http://fsoa.org.uk/

The Business Continuity Institute www.thebci.org

Preparing for Emergencies
www.gov.uk

London Prepared
www.london.gov.uk

Security Industry Authority
www.sia.homeoffice.gov.uk

Anti Terrorist Branch Hotline: 0800 789 321 -

Acknowledgments

With thanks to the following for their knowledge, expertise and time

Centre for the Protection of the National Infrastructure (CPNI)
Metropolitan Police Service (SO13) Security Co-ordinators
HOK Sport Architecture
Scottish Exhibition and Conference Centre
The England and Wales Cricket Board
The Football League
The Rugby Football Union
The Rugby Football League
The Football Licensing Authority
The Football Safety Officers Association
The Cricket Safety Officers Association
The Rugby League Ground Safety Officers Association
Surrey County Cricket Club for providing images of the Brit Oval