NaCTSO
National Counter Terrorism Security Office

ASSOCIATION OF CHIEF POLICE OFFICERS

Counter-Terrorism Security Advice for *Hazardous Sites*

This is an 'image-free' document of a full colour booklet which will be issued in due course, but in the interim may be shared with relevant sites in your area.

Foreword

Sites storing hazardous chemicals or dangerous sources pose significant risks to the protection of the public. Most sites storing significant quantities of such substances are regulated under the Control of Major Accident Hazards Regulations (COMAH), implementing the Seveso Directive applicable across European Union member states. COMAH sets high standards for control of risks to health, safety and environment and require sites to be safely managed, operated and maintained to minimise the risk of accidents. However, accidental releases are not the only risks at such sites. Terrorists may seek to exploit security vulnerabilities to attack these sites in a way that leads to a catastrophic release, or alternatively, may seek to obtain chemicals stored at the site in order to commit an attack elsewhere.

Such an attack could have potentially catastrophic consequences. This document is designed to help sites look at their practices and procedures and to help them identify and to take action to reduce vulnerabilities, thereby lessening the risks to their site. Such measures need not be expensive. Putting into place good practice can help to make a target less attractive to a terrorist. The risks from terrorism cannot be reduced to zero but this booklet is designed to encourage simple measures to be put into place to reduce that risk to as low as reasonably practicable.

The consequences arising from a terrorist attack on a hazardous chemicals site are so large that action must be taken to lessen this risk as far as is possible.

This document had been produced with the assistance of the Centre for the Protection of National Infrastructure (CPNI), the Office for Security and Counter Terrorism (OSCT) at the Home Office, the Department for Business, Innovation and Skills (BIS), the Department for Energy and Climate Change, the

Department for Transport (D*f*T), the Health and Safety Executive (HSE) , the Chemical Industries Association and the Chemical Business Association.

Contents

one introduction

This guide is intended to give protective security advice to those who are responsible for the security of facilities, sites, and plants storing, producing, or using hazardous chemicals or dangerous sources irrespective of size and capacity. It is aimed at sites 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 site 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 at the site. 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 threats or hoaxes designed to frighten and intimidate. Sites with hazardous materials may also be at risk of theft by terrorists seeking to use those materials in attacks carried out elsewhere.

Major accidents around the world, including incidents in the UK such as at Flixborough in 1974 and at the Buncefield terminal in 2005, demonstrate the potential impact that explosions at some major hazard sites could cause. These were very serious incidents, and in the case of Flixborough resulted in multiple fatalities amongst many other consequences. Although these were accidents following which lessons have been learned and legislation has changed, the potential remains for a terrorist to achieve the same or similar effect.

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.

This document is not 'site specific' and recognises that all sites, facilities and plants are different. It is also recognised that some of the guidance included in this document may

have already been introduced by various sites, such as those storing radioactive sources, or pathogens and toxins, where there is specific regulation or legislation covering security measures.

For specific advice relating to your site, contact the nationwide network of specialist police advisers known as Counter Terrorism Security Advisers (CTSAs) through either your local police service or the National Counter Terrorism Security Office (NaCTSO) at www.nactso.gov.uk . NaCTSO is responsible for co-ordinating the work of CTSAs.

REMEMBER!
Effective management of safety and security should be complementary priorities for major hazard sites

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

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

[Back to 'Contents']

two managing security risks

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

Management already have responsibilities for employee and public protection under health and safety legislation, to prevent major accidents and minimise the consequences from any that do occur under the Control of Major Accident Hazards (COMAH) and the Control of Substances Hazardous to Health (COSHH) regulations. (See guidance published by the Health and Safety Executive (HSE) www.hse.gov.uk/coshh/)

All sites storing or handling specified quantities of certain chemicals of a hazardous nature are regulated by the COMAH regulations and depending on the quantity of the hazardous materials stored or used, will produce either a stand-alone Major Accident Prevention Policy (MAPP) or a full safety report, which includes the MAPP. Many sites will fall within the scope of the provisions of the domestic and international transport regulations for the carriage of dangerous goods which also have provisions affecting sites and in defined cases security plans and specific allocation of responsibilities for security to competent and qualified persons with the appropriate authority to carry out their responsibilities.

The Health and Safety Executive (HSE), the Environment Agency (EA), the Scottish Environmental Protection Agency (SEPA), the Health and Safety Executive Northern Ireland (HSENI) and Natural Resources Wales (NRW) comprise the joint COMAH Competent Authority (CA) and are responsible for the enforcement of the COMAH regulations. The Department for Transport (DfT) is the Competent Authority for the enforcement of the 'Carriage of Dangerous Goods' regulations.

Law, Liability and Insurance

There are legal and commercial reasons why your security plan should deter such acts, or at least minimise their impact. They are:

Criminal prosecution and heavy penalties under health and safety laws for companies and individuals who manage sites are a real possibility in the wake of either an accident or a terrorist incident should there be a breach of relevant legislation. Especially relevant to protective security are specific requirements under health and safety at work legislation and regulations to do the following:

• **Carry out adequate risk assessments** and put suitable measures in place to manage identified risks within their direct control and to mitigate the possible consequences of external risks; then be alert to the need to conduct prompt and regular reviews of those assessments and measures in the light of new threats and developments.

• **Co-operate and co-ordinate** safety arrangements between owners, managers, security staff, tenants and others involved on site, including the sharing of incident response plans and working together in testing, auditing and improving planning and response. In some areas where there are hazardous sites in close proximity there is the potential for a 'domino' effect.

• **Ensure adequate training, information and equipment** are provided to all staff, and especially to those involved directly in safety and security.

• Put proper procedures and competent staff in place to deal with incidents which might cause **imminent and serious danger** and/or, require evacuation of the premises.

Insurance against damage to your own site from terrorist acts is generally available but typically at an additional premium. Adequate cover for loss of revenue and business interruption during a rebuild or decontamination is expensive even where available from the limited pool of specialist underwriters. Full protection against compensation claims for death and injury to staff, contractors, and customers caused by terrorism is achievable, albeit at a cost.

With individual awards for death and serious injury commonly exceeding the publicly funded Criminal Injuries Compensation Scheme upper limit, there is every incentive for victims to seek to make up any shortfall through direct legal action against owners, operators, managers and tenants under occupiers liability laws.

Business continuity

Business continuity planning is essential in ensuring that your organisation can cope with an incident or attack and return to '**business as usual**' as soon as possible. Following the Buncefield incident many companies and businesses were still unable to return over a year after the explosion. An attack on a crucial contractor or supplier can also impact on business continuity. You can develop a basic plan, which can be implemented to cover a wide range of possible actions. For example, part of the plan will cover evacuation procedures, but the principles will be generally applicable regardless of the type of incident. This is particularly relevant for smaller operations that may not have the resources to withstand even a few days financial loss. See Appendix A – Business Continuity checklist.

There is an International Standard - ISO 22301 - which provides further guidance on the subject of Business Continuity Plans.

Reputation and goodwill are valuable, but prone to serious and permanent damage if it turns out that you gave a less than robust, responsible and professional priority to best protecting people against attack. Being security minded and better prepared reassures your staff and customers that you are taking security issues seriously and could potentially deter an attack.

Do you know who your neighbours are and the nature of their business? Could an incident at their premises affect your operation? There is limited value in safeguarding your own premises in isolation. Take into account your neighbours' business plans and those of the emergency services. In some areas where there are hazardous sites in close proximity there is the potential for a 'domino' effect, particularly in the oil industry where a hydrocarbon explosion at a plant could lead to an explosion at another, nearby plant.

Assess the security risks

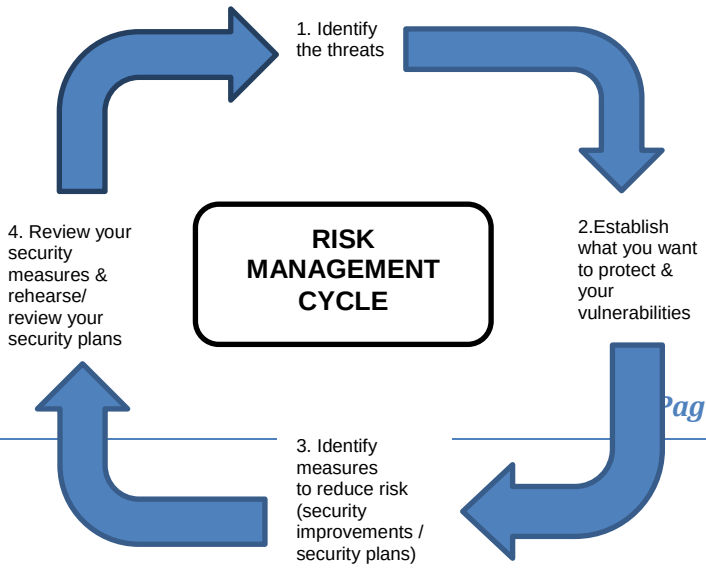
Measures you may consider for countering terrorism will also usually be effective against other threats, such as theft and burglary. Any extra measures that are considered should integrate wherever possible with existing security.

For some sites, simple good practice - coupled with vigilance and well exercised contingency arrangements - may be all that is needed. If, however, you assess that you are vulnerable to attack, you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable. With regard to protective security, the best way to manage the hazards and risks to your site 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.

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 site, staff or activities that would particularly attract a terrorist attack or materials which terrorists might seek to obtain?
- Is there an association with high profile individuals or organisations which might be terrorist targets?
- Does your location mean that you may suffer business disruption from an attack or other incident involving 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?
- 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 contractors, and visitors)
- Physical assets (the fabric of your site and its contents, including the hazardous materials held on site)
- Information (electronic and non-electronic data)
- Processes (supply chains, 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 on-going research.

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 site e.g. fire, accidents, 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 site 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 aware? How good are your staff at spotting unusual activity? (See Hostile Reconnaissance on page 60).

Step Three: Reduce the 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 may be unaware of existing security measures, or may have developed habits to circumvent them. Simply implementing 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 accurate, workable and up to date. You should be aware of the need to modify them to take into account any changes in your site (e.g. new building work, changes to personnel, information and communication systems and revised health and safety practices).

Rehearsals and exercises should, wherever possible, be conducted in conjunction with the emergency services and local authority. You could also consider including exercising responses to malicious acts as well as accidents.

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.

REMEMBER: THE GREATEST RISK TO ANY ORGANISATION IS COMPLACENCY.

[Back to 'Contents']

three security planning

If you do not have one already, you should appoint one person to take the lead responsibility for security, this is also a requirement of the transport regulations for sites holding larger quantities of high consequence dangerous goods. This 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.

They must be involved in the planning and design of the site's exterior security, access control etc. so that the terrorist dimension is taken into account. The individual allocated with a security oversight must similarly be consulted over any new building or renovation 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 Security Manager, or other individual with security oversight, should have responsibility for the following key areas:

- Production of the security plan based on the risk assessment
- Formulation and maintenance of a search plan
- Formulation and maintenance of contingency plans
- Liaising with the police, other emergency services and local authorities
- Arranging staff training and conducting briefings / debriefings
- Conducting regular reviews of the plans

For independent and impartial counter terrorism advice and guidance that is site specific, the individual with responsibility for security should establish contact with the local police Counter Terrorism Security Adviser (CTSA) (www.nactso.gov.uk).

Your CTSA can:

- Help you assess the risk, 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
- Provide information on professional bodies representing installers of such equipment
- Arrange for suitably qualified advisers to assist with search plans

During the development and review of plans it is also advisable to discuss them with any other occupants of the site, as well as to consult the emergency services and your local authority.

Creating your Security Plan

The site should 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. telephone bomb threat)
- Instructions on how to respond to the discovery of a suspicious item or event
- Search plan
- Evacuation plans and details on securing the site in the event of a full evacuation
- Business continuity plan
- Communications and media strategy which includes handling enquiries from concerned family and friends
- Keeping it up-to-date
- Retaining it securely

Your plan 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.

[Back to 'Contents']

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 the safety of staff, contractors, or visitors.

Your risk assessment will determine which measures you should adopt, but they range from basic good housekeeping 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.

Implementation of successful security measures requires:

- 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 Adviser (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 also 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 ALL staff (including contractors) 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 site.

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 in the site by strangers. See Hostile Reconnaissance on page 60.

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 18.

Security passes

If a staff pass system is in place, insist that staff wear their 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 can be a significant deterrent to terrorists and may be a suitable protective security consideration for your premises.

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 30.

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 buildings.

For site specific advice and guidance you should contact your local police Counter Terrorism Security Adviser (CTSA) either through your local police or the NaCTSO website www.nactso.gov.uk. See also Vehicle Borne Improvised Explosive Devices on page 52.

Doors and windows

Doors and windows of the appropriate standard 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. In some cases such protection may already be in place as a result of measures introduced to comply with other health and safety requirements, such as Occupied Buildings Risk Assessment which requires companies to assess risk from potential major accidents and to implement measures to protect people from injury including from flying glass.

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 (www.acpo.police.uk). For further information, contact the Alarms Administration Office at your local police headquarters.

The alarm system at sites within Scotland should be compliant with the Police Service of Scotland's Remote Alarms Standard Operating Procedure (available from http://www.scotland.police.uk/access-to-information/policies-and-procedures/police-scotland-policies/ or alternatively advice can be obtained from CTSAs).

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.

See CCTV guidance on page 20.

[Back to 'Contents']

five access control

There should be clear demarcation between public and private areas, with appropriate access control measures into and out of the private side. There should additionally be clear demarcation and appropriate controls within private areas where only limited members of staff are allowed access to areas containing the hazardous materials.

Risk assessment

Refer to 'managing the risks' on page 6 and decide the level of security you require before planning your Access Control system. Take into account any special features you may require.

Appearance

Your Access Control system is often the first impression of security made on visitors to your site.

Ease of access

Examine the layout of your system. Do your entry and exit procedures allow legitimate users to pass without undue effort and delay?

Training

Are your staff fully aware of the role and operation of your Access Control system? Your installer should provide adequate system training.

System maintenance

Your installer should supply all relevant system documentation, e.g. log books and service schedules. Are you aware of the actions required on system breakdown? Do you have a satisfactory system maintenance agreement in place?

Interaction

Your Access Control system may supplement other security measures. Consider system compatibility.

Compliance

Are you compliant with current legislation and regulations with respect to human rights and health and safety?

These are important to ensure access does not discriminate against particular groups, such as ensuring 'swipe' entry systems are at the correct height to be used by wheelchair users, and to ensure that any data held or gathered is maintained and handled appropriately.

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 the intent is to deliver explosives to the site via person, car or lorry, or to steal hazardous or dangerous materials, a terrorist needs physical access in order to reach the target.

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

[Back to 'Contents']

six cctv guidance

CCTV can help clarify whether a security alert is real and is often vital in any post incident investigation.

You should constantly monitor the images captured by your CCTV system or regularly check recordings for suspicious activity ensuring at all times full compliance with the Data Protection Act 1998 which should be specified in your CCTV Data Protection Policy.

Since 20th March 2006, contract CCTV operators must carry an SIA CCTV (Public Space Surveillance) licence - it is illegal to work without one. Your security contractor should be aware of this and you should ensure that only licensed staff are supplied if the 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 activity of particular people, either by controlling 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

CCTV cameras should, if possible, cover all the entrances and exits to your premises and other areas that are critical to the safe management and security of your commercial centre. This could include areas storing of bulk chemicals.

With more organisations moving towards digital CCTV systems, you should liaise with your local police to establish that your system software is compatible with theirs to allow retrieval and use of your images for evidential purposes.

The Centre for applied Science and Technology (CAST) has published many useful documents relating to
CCTV including 'CCTV Operational Requirements Manual' (Ref: 17/94), 'UK Police Requirements for Digital CCTV Systems' (Ref: 09/05), 'Performance Testing of CCTV Systems' (Ref: 14/95), and
'CCTV Control Room Ergonomics' (Ref: 14/98).

CAST has a page on the UK government website which has many useful documents relating to technological solutions for crime prevention. CAST can be found at:
https://www.gov.uk/government/organisations/home-office/series/centre-for-applied-science-and-technology-information

Consider also the following points:

- Ensure the date and time stamps of the system are accurate
- Regularly check the quality of recordings
- Digital CCTV images should be stored in accordance with the evidential needs of the Police.

  Refer to HOSDB publication 09/05 - UK Police Requirements for Digital CCTV Systems.
- Ensure that appropriate lighting complements the system during daytime and darkness hours
- For analogue systems change tapes daily – use no more than 12 times
- Keep your tapes for at least 31 days
- Use good quality video tape and check it regularly by playing it back on a different machine
- Ensure 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 'D'.

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

[Back to 'Contents']

seven secure storage of chemicals

This section is drawn largely from the booklet 'Secure Your Chemicals', and which can be obtained from: www.sea.org.uk/home/news?view=show&content_id=373

The control and accountability of hazardous substances is viewed as a crucial element of good practice. There are many valid reasons why all those who come into contact with hazardous chemicals should maintain tight controls on the type of chemical, how much they have and ensure that it is stored in a safe and secure manner with access restricted. Such chemicals are usually expensive and carry high risks such as toxicity, flammability or volatility, either on their own or when mixed with other chemicals.

There are three key areas that need to be considered. These are:

- **Limit the number of people who have access**
- **Ensure you have physical security measures**
- **Keep an audit trail from delivery to use/disposal**

CURRENT LEGISLATION

The main regulation affecting the handling and use of hazardous substances is found under the Control of Substances Hazardous to Health Regulations 2002 (COSHH – as amended). COSHH requires employers to prevent or control the exposure to hazardous substances at work, to prevent ill health.
(www.hse.gov.uk/coshh/basics/substance.htm)

Larger sites may be captured by the Control of Major Accident Hazards (COMAH) regulations. These regulations require operators to take all measures necessary to prevent major accidents and to limit the consequences to people and the environment where they do occur. Separate guidance regarding chemical storage, including the use of cages and the separation of some chemicals is available. For further information see www.hse.gov.uk/chemicals.

The Health and Safety At Work etc. Act, 1974 requires employers and the self-employed to protect the health and safety of their employees and others, where it involves the storage, handling and use of potentially dangerous substances. This includes the prevention of the acquisition, possession and use of substances where there is specific

legislation banning their use. Guidance on the workings of the Health and Safety At Work etc. Act, 1974 can be found at www.hse.gov.uk/legislation/hswa.htm

The Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) Regulations were introduced in 2007. They aim to:

- Provide a high level of protection for human health and the environment regarding the use of chemicals.
- Make people who place chemicals on the market (manufacturers and importers) responsible for understanding and managing risks associated with their use and the cascading of pertinent information on the substances up and down the supply chain.

For further information see www.hse.gov.uk/coshh and www.hse.gov.uk/reach

Certain very hazardous chemicals are subject to licensing controls under the Chemicals Weapons Act 1996. The licensing regime applies to the production, use, possession, import or export of such chemicals. A schedule to the Act lists the specific chemicals to which the licensing controls apply. There are restrictions on activities involving these chemicals and limits on the quantity of chemicals that can be produced or stored. Licence holders need to undertake a risk assessment, ensure measures are in place to address security and safety risks, keep records and have effective waste disposal measures in place.

The Chemical Weapons Act 1996 also includes powers to ensure compliance with the Chemical Weapons Convention by those subject to licensing controls. The Act requires companies to provide data and authorises the inspection of sites which work with certain toxic chemicals in order to build confidence that such chemicals are not being misused. DECC is the National Authority responsible for implementation of the CWC in the UK.

For further information see:
http://tools.decc.gov.uk/en/content/cms/meeting_energy/en_security/nonprolif/chemical_bio/cwc_uk_auth/cwc_uk_auth.aspx

MANAGEMENT RESPONSIBILITIES

It is the responsibility of the management at any site that holds hazardous chemicals, for whatever reason, to ensure that they are procured, stored, used and disposed of in a safe and secure manner. This needs to be supported by restricting the number of persons who have access to such substances and by good record keeping. This will ensure that you can account for all your chemicals at all times.

It is essential that all those who have been granted access to chemicals fully read and understand the safety data sheets supplied with them. 'Know Your Customer' principles should also be followed so that suspicious purchases may be picked up and the relevant authorities advised so that action may be taken. Further information and posters for 'Know Your Customer' can be obtained from www.nactso.gov.uk

ASSESS WHAT YOU HAVE

Identify hazardous substances

What may appear to be harmless to some users could be seen as a significant hazard to others, especially if it becomes more dangerous when mixed with other substances. This includes precursor chemicals that could be used to make drugs or explosives, as well as other substances that, when mixed, could produce toxic gases. If your company or organisation is holding such chemicals, they need to be identified by a designated and suitably qualified member of staff and kept in appropriate conditions. Guidance can be found at www.hse.gov.uk/chemicals.

If you are unsure, look at the company's COSHH assessment information or contact the company that supplied the chemicals and ask for suitable safety datasheets to be provided. Further information can be obtained from one of the organisations listed at the end of this section.

Identify risks

As well as the security of the chemicals you hold or use on site external factors can also have a significant effect on the overall security of your chemicals. For example, your site will be at a higher risk of intrusion for theft if you store other commodities on site such as valuable scrap metals or chemicals which are currently in short supply.

Questions you should therefore consider are:

- Can you store your chemicals in secure storage?
- How good are your site security measures?
- Has your site suffered from any incidents before?
- Are there other 'desirable' materials on your site (such as metals or vehicle fuels)?

Quantity on site

It is important to know exactly how much of each chemical you have on your site. It should be kept in a manner according to HSE guidance www.hse.gov.uk/chemicals. Questions you should consider are:

- How much of any one chemical do you have on site at any one time?
- How often do you conduct a stock check?
- Could you reduce the quantities held or use less hazardous alternatives?
- Are they kept in accordance with regulations/guidance/standards?

Storage

Hazardous chemicals held in storage must be closely monitored and, if necessary, circulated, to ensure they do not go beyond their useful life. Questions that you should consider are:

- Have you complied with HSE guidance?
- Is there a system to circulate substances so that they don't become out of date?
- Is there a full audit list available of what you have and where it is held?
- Can you isolate bulk stock and lock it away until it is needed?

Use

When chemicals are removed from storage for use, it becomes more important to know exactly how much has been removed and that the exact amount removed has been used. Questions you should consider are:

- Who uses the hazardous chemicals and are they properly trained?
- Do they maintain an audit trail of how much is used and when?
- Is this witnessed by a supervisor?

Laboratories

Some larger sites will probably have their own testing laboratory on site. This code applies equally to even small amounts of chemicals.

Disposal

Many hazardous chemicals can still be a danger, even when they have been used in a process and all that is left is a residue. This legally counts as hazardous (or Special in Scotland) waste (unless made inert). Questions you should consider are:

- How do you dispose of unwanted hazardous chemicals?
- Is there an audit trail? Is it witnessed?
- How are hazardous chemicals stored before disposal?
- Have you used a correctly qualified disposal service?

There are some 'companies' operating illegally in the UK. If in doubt, check phone numbers, websites etc to ensure you are dealing with a qualified hazardous waste company. If your hazardous waste is illegally dumped, you could be liable for it and any consequences.

ACTION

From the moment a hazardous chemical arrives on your site, you must be able to demonstrate full **CONTROL** of the chemical, and be able to **ACCOUNT** for it at all times, until its use or final disposal.

Having assessed **what** you have, **how much** you have and **where** it is, you now need to take action to place controls in the three key areas. The main focus for these controls should be procedural with good regular record keeping.

This is usually focused on restricting the number of people who have access to hazardous chemicals. Control measures can be imposed by:

- Physical measures
- People
- Procedures

More detail on each of these is given below, and within the relevant sections of this booklet (see Section 4 Physical Security, Section 5 Access Control, Section 6 CCTV Guidance, and Section 12 Personnel Security).

Physical measures

Physical security controls do not have to cost a lot of money or generate a significant inconvenience. They range from simple locks to expensive electronic security equipment. Sometimes you may be able to use equipment that is already on site. For site specific advice and guidance you should contact your police Counter Terrorism Security Adviser (CTSA) either through your local police or the NaCTSO website www.nactso.gov.uk. Such measures include:

- Good quality doors, windows and the frames that hold them
- Solid or reinforced walls
- Strong locking devices that are bolted into place
- A security alarm
- Good lighting at night, which could be supported by CCTV
- Use of equipment you already have, but concentrated in a small designated area

People

Regardless of how good your physical security measures are, poor practice by staff members can result in doors not being locked or hazardous materials being left in vulnerable places. The fewer people who have access to hazardous substances, the fewer people you will have to advise or train. Consider the following:

- Minimise the number of people who have access to hazardous chemicals
- Ensure these people are trustworthy and correctly trained
- Ensure they have the knowledge and means to maintain audits at all times
- Provide them with a manager who they can confide in if they have problems, without fear of criticism or punishment

Procedures

Record keeping is essential for companies to be fully accountable, so that they can clearly demonstrate exactly what they are holding and in what quantities, at any given time. An audit trail must include:

- What is delivered, when it is delivered, where it is stored, when it is used (or disposed of) and at what quantities
- Totals held in stock and quantities withdrawn for use and verification of its use
- The ordering of chemicals must be limited to essential and authorised personnel only, and is optimised so that stocks are kept as low as reasonably possible
- The onward sale of chemicals should only be conducted in exceptional circumstances when you are in absolutely no doubt who the customer is, and that they have a lawful reason to possess such chemicals
- For more information regarding what would constitute a suspicious order, please see the 'Know Your Customer' advice available through www.nactso.gov.uk

Report

If you discover that hazardous chemicals are missing from your company or you have identified suspicious behaviour relating to such chemicals, you must take the following action:

- Double check that stock is missing by enquiring with all staff members
- Record as much detail as possible about missing stock or a suspicious incident Include names, times, dates and list the name and quantities of the chemicals missing/ordered.
- If for any reason you believe that a suspicious incident could be related to terrorism, contact the anti-terrorist hotline on **0800 789321**

Good Practice

Simple methods can be used to measure the contents in storage. This includes weighing smaller packages or using a dip stick in larger receptacles and tanks. Ensure inlets and outlets are secured and sealed using locks and/or anti-tamper ties. Keep records of the serial numbers.

Hazardous chemicals are usually sold by reputable companies who belong to one of the main professional associations such as the Chemical Business Association (CBA) or the Chemical Industries Association (CIA).These associations have strict Codes of Conduct which ensure their members behave in a lawful and responsible manner. If you are approached by a company selling hazardous substances and you feel it may be suspicious you can check whether the company is a member of either of these associations through their websites (see below). Further 'Know Your Customer'

information as well as downloadable posters to help remind your staff can also be found on the NaCTSO website.

Further information

If you are looking for further advice, the following agencies and websites have a wealth of information. You are strongly advised to look at these:

Health and Safety Executive – www.hse.gov.uk

Surface Engineering Association – www.sea.org.uk

Chemical Business Association – www.chemical.org.uk

Chemical Industries Association – www.cia.org.uk

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

Environment Agency – www.environment-agency.gov.uk

Health and Safety Executive Northern Ireland – www.hseni.gov.uk

Natural Resources Wales – www.naturalresourceswales.gov.uk

Scottish Environmental Protection Agency – www.sepa.org.uk

[Back to 'Contents']

eight search planning

Searches of sites should be conducted as part of routine procedure to identify unexplained items or people or, for example, perimeter fence gaps but the Security Manager should also have search plans prepared to be conducted in response to a specific threat or when there is a general alert of attack.

The following advice is generic for most sites, but recognises that sites are built and operate differently. If considered necessary advice and guidance on searching should be available from a Police Search Adviser (POLSA) which can be arranged through your local CTSA contacted directly through your local police force or through NaCTSO at www.nactso.gov.uk.

Search Plans

- Search plans should be prepared in advance and staff should be trained to them.
- The conduct of searches will depend on local circumstances and local knowledge, but the overall objective is to make sure that the entire premises and grounds are searched in a systematic and thorough manner so that no part is left unchecked.
- If you decide to evacuate your site in response to a threat, you may also need to consider a search in order to ensure it is safe for re-occupancy.
- The police will not normally search sites. They are not familiar with the layout and will not be aware of what should be there and what is out of place. They cannot, therefore, search as quickly or as thoroughly 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, searching should be conducted in pairs; to ensure a systematic and thorough approach.

Action You Should Take

Divide your site into sectors. If the site is organised into different operating areas, these should be identified as separate search sectors. Each sector must be of manageable size.

The search plan should have a written checklist for each sector- signed as completed for the information of the Security Manager and Police Commander.

Remember to include canteen and relaxation areas, 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 an internal PA 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. Consider making detailed notes or a sketch whilst you are awaiting police attendance

The Security Manager 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.

If you don't have any procedures for dealing with unattended items then you could consider using the HOT protocol. Is the item **Hidden**? Is it **Obviously Suspicious**? Is it **Typical** of what you normally see on your site? This could give you a clear structure to identify quickly if something is lost property, discarded rubbish or is, in fact, a genuinely suspicious item. Remember, some terrorists do not want to be seen or noticed or to have their IEDs discovered prior to functioning.

The HOT protocol was originally devised by the British Transport Police for use in the mass transit rail environment, and has been used very successfully by them and rail staff for almost 20 years.

See Good Practice Checklist – Searching in Appendix 'E'.

[Back to 'Contents']

nine good housekeeping

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

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

- Avoid the use of litter bins around the site if possible, (but if you do this ensure that there is additional and prompt cleaning)
- The use of clear bags for waste disposal is an alternative as it provides an easier opportunity for staff to conduct an initial examination for suspect articles
- Review the use and security of compactors, wheelie bins and metal bins to store rubbish within sites 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 suspect articles
- Lock unoccupied offices, rooms and store cupboards
- Ensure that everything has a place and that things are returned to that place
- Put seals on maintenance hatches
- Keep external areas as clean and tidy as possible
- All sites should have in place an agreed protocol for the security of outside 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 site security in advance
- Pruning all vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any suspect articles

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 site CCTV system to ensure that it has sufficient coverage both internally and externally

• Site management should identify a secondary secure location for a Control Room as part of their contingency plans

• Security systems that are reliant on power should have an Uninterrupted Power Supply (UPS) available and regularly tested.

See Good Practice checklist – Housekeeping in Appendix 'B'.

[Back to 'Contents']

ten mail handling

Most sites and businesses receive large amounts of mail and other deliveries and this offers an attractive route into your premises for terrorists. The Centre for the Protection of National Infrastructure (CPNI) offers advice on screening mail and deliveries, which can be found 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 attack method. 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 oddly 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, rotten. 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.

• 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.

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 on the threat and on defensive measures from your local police Counter Terrorism Security Adviser (CTSA) contacted directly through your local police force or through NaCTSO at www.nactso.gov.uk.

• 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.

• 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 scanners may detect devices for spreading chemical, biological, and radiological (CBR) materials (e.g. explosive devices), they will not detect the materials themselves.

• 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 who are 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.

[Back to 'Contents']

eleven evacuation planning and protected spaces

As with search planning, evacuation should be part of your security plan. You might need to evacuate your site because of:

- **A threat received directly by your site**
- **A threat received elsewhere** and passed on to you
- **Discovery of a suspicious item to the site** (perhaps a postal package, an unclaimed hold-all or rucksack)
- **Discovery of a suspicious item or vehicle outside the building**.
- **An incident** to which you have been alerted

Whatever the circumstances, you should tell the police as soon as possible what action you are taking.

The biggest dilemma facing anyone responsible for an evacuation plan is how to judge where the safest place might be. For example, if an evacuation route takes people past a suspect article outside your building, or through an area believed to be contaminated, external evacuation may not be the best course of action.

A very important consideration when planning evacuation routes in response to near simultaneous terrorist attacks is to ensure people are moved away from other potential areas of vulnerability, or areas where a larger secondary device could detonate.

The decision to evacuate will normally be yours, but the police will advise. In exceptional cases they may insist on evacuation, although they should always do so in consultation with your Security Manager.

A general rule of thumb is to find out if the device is external or internal to your premises. If it is within the building you may consider evacuation, but if the device is outside the building it may be safer to stay inside.

Planning and initiating evacuation should be the responsibility of the [Security Manager]. Depending on the size of your premises and the location of the building, the plan may include:

- Full evacuation outside the building
- Evacuation of part of the building, if the device is small and thought to be confined to one location (e.g. a small bag found in an area easily contained)
- Full or partial evacuation to an internal safe area, such as a protected space, if

available

- Evacuation of all staff apart from designated searchers

Evacuation

Evacuation instructions must be clearly communicated to staff and routes and exits must be well defined. People must be appointed to act as marshals and as contacts once the assembly area is reached. Assembly areas should be at least 500 metres away from the incident. In the case of most vehicle bombs, for instance, this distance would put them beyond police cordons - although it would be advisable to have an alternative about 1km away. As far as possible sites should be aware of other potential targets in the area and where there are 'cluster sites' evacuation plans could be considered in co-ordination with other businesses. This is frequently the case with city centres.

It is important to ensure that staff are aware of the locations of assembly areas for incident evacuation as well as those for fire evacuation and that the two are not confused by those responsible for directing visitors to either.

Grab bags

A 'Grab Bag' should be available which contains essential equipment and information. All relevant contact information, the staff involved, tenants and other site information should be contained in an easily accessible format.

Suggested 'Grab Bag' contents:

Documents:

• Business Continuity Plan - your plan to recover your business or organisation
• List of employees with contact details - include home and mobile numbers. You may also wish to include next-of-kin contact details
• Lists of customer and supplier details
• Contact details for emergency glaziers and building contractors
• Contact details for utility companies
• Building site plan, including location of gas, electricity and water shut off points
• Latest stock and equipment inventory
• Insurance company details
• Local authority contact details

Equipment:

• Computer back-up tapes / disks / USB memory sticks or flash drives
• Spare keys / security codes
• Torch and spare batteries
• Hazard and cordon tape
• Message pads and flip chart
• Marker pens
• General stationary
• Mobile telephone with credit available, plus charger
• Dust and toxic fume masks
• Camera

Make sure this pack is stored safely and securely off-site (in another location). Ensure items in the pack are checked regularly, are kept up to date, and are working. Remember that cash / credit cards may be needed for emergency expenditure.

This list is not exhaustive, and there may be other documents or equipment that should be included for your business or organisation.

Car parks should not normally be used as assembly areas, as they may be used by terrorists to place secondary devices and furthermore, assembly areas should always be searched before they are used. Car parks situated within protectively secured areas may be acceptable.

Disabled staff should be individually briefed on their evacuation procedures.

In the case of suspected:

Letter or parcel bombs

If in a premises, evacuate the room and the floor concerned along with the two floors immediately above and below.

Chemical, Biological and Radiological Incidents

Responses to CBR incidents will vary more than those involving conventional or incendiary devices, but the following general points should be noted:

- The exact nature of an incident may not be immediately apparent. For example, an IED might also involve the release of CBR material.
- In the event of a suspected CBR incident within a building, switch off all air-conditioning, ventilation and other systems or items that circulate air (e.g. fans and personal computers). Do not allow anyone, whether exposed or not, to leave evacuation areas before the emergency services have given medical advice, assessments or treatment.
- If an incident occurs outside an enclosed temporary structure or building, close all doors and windows and switch off any systems that draw air into the structure/building.

Agree your evacuation plan in advance with the police and emergency services, the local authority and any neighbours. Ensure that staff with particular responsibilities are trained and that all staff are drilled. Remember, too, to let the police know what action you are taking during any incident.

Security managers should ensure that they have a working knowledge of the heating, ventilation and air conditioning (HVAC) systems and how these may contribute to the spread of CBR materials within the building.

Protected Spaces

Protected spaces may offer the best protection against blast, flying glass and other fragments. They may also offer the best protection when the location of the possible bomb is unknown, when it may be near your external evacuation route or when there is an external CBR attack.

Since glass and other fragments may kill or maim at a considerable distance from the centre of a large explosion, moving staff into protected spaces is often safer than evacuating them onto the streets. Protected spaces should be located:

- In areas surrounded by full - height masonry walls e.g. internal corridors, toilet areas or conference rooms with doors opening inwards
- Away from windows and external walls
- Away from the area in between the building's perimeter and the first line of supporting columns (known as the 'perimeter structural bay')
- Away from stairwells or areas with access to lift shafts where these open at ground level onto the street, because blast can travel up them. If, however, the stair and lift cores are entirely enclosed, they could make good protected spaces.
- Avoiding ground floor or first floor if possible
- In an area with enough space to contain the occupants

When choosing a protected space, seek advice from a structural engineer with knowledge of explosive effects and do not neglect the provision of toilet facilities, seating, drinking water, lighting and communications.

Consider duplicating critical systems or assets in other buildings at a sufficient distance to be unaffected in an emergency that denies you access to you own. If this is impossible, try to locate vital systems in part of your building that offers similar protection to that provided by a protected space.

Communications

Ensure that staff know their security roles and that they or their deputies are always contactable. All staff, including night or temporary staff, should be familiar with any telephone recording, redial or display facilities and know how to contact police and security staff in or out of office hours.

It is essential to have adequate communications within and between protected spaces. You will at some stage wish to give the 'all clear', or tell staff to remain where they are, to move to another protected space or evacuate the building. Communications may be by public address system (in which case you will need standby power), hand-held radio or other standalone systems. Do not rely on mobile phones. You also need to communicate with the emergency services. Whatever systems you choose should be regularly tested and available within the protected space.

Converting to open plan

If you are converting your building to open plan accommodation, remember that the removal of internal walls reduces protection against blast and fragments.

Interior rooms with reinforced concrete or masonry walls often make suitable protected spaces as they tend to remain intact in the event of an explosion outside the building. If corridors no longer exist then you may also lose your evacuation routes, assembly or protected spaces. Any new layouts or alterations to existing layouts require a review of your bomb threat contingency procedures.

When making such changes, try to ensure that there is no significant reduction in staff protection, for instance by improving glazing protection. If your premises are already open plan and there are no suitable protected spaces, then evacuation may be your only option.

See Evacuation Good Practice checklist at Appendix F.

[Back to 'Contents']

twelve 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 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.

Much of the following advice simply reflects 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 and 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 to safeguard national security if the individual wants to be employed by particular organisations such as the UK Atomic Energy Authority - employers 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 reasonably good quality false documentation on the Internet has made establishing identity more of 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 the 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 risks and, as far 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
- Restrict 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. On-going 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 changes or disappointments
- Manifestations of stress such as over-emotional behaviour
- Unusual interest in security measures or areas of work outside the normal remit
- Changes in working patterns, for instance working alone or at unusual hours, failing to take holidays
- Frequent unexplained absences
- Repeated failure to follow recognised procedures
- Unusual travel abroad
- Relationships with or support for individuals or institutions that are generally regarded as professionally suspect
- Sudden or marked change in religious, political or social affiliation or practice which has an adverse impact on the individual's performance or attitude to security.

Individual cases will have unique features and it may take a combination of behaviours and attitudes to warrant further concern. It is important to note that some of these signs may be the result of ill-health. You should allow for this in your consideration of them.

You may also wish to consider whether to undertake checks for existing staff where this has not already been done to a satisfactory level. If you have serious reason to suspect that you are being bugged or subject to other forms of electronic 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 you should 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, 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 ill; 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

• 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 – Personnel Security in Appendix 'G'.

[Back to 'Contents']

thirteen 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 noticeboards, using secure cabinets, locking appropriate doors and giving guidance to staff, especially those who have to take information off the premises.

Electronic attack

Electronic 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. Electronic attacks are much easier when computer systems are connected directly or indirectly to public networks such as the internet.

The typical methods of electronic 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 an electronic 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 an electronic 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 Personnel Security on page xx)
• Consider encryption packages for material you want to protect, particularly if taken offsite – 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 CPNI website which identifies the top twenty critical controls for cyber defence. These are a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence. http://www.cpni.gov.uk/advice/cyber/Critical-controls/

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 rip 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 electronic media, such as overwriting and degaussing. For further information visit www.mi5.gov.uk

Before investing in waste destruction equipment you should:

• If you use contractors, ensure that their equipment and procedures are sufficient. 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 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 'H'. [Back to 'Contents']

fourteen 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. Sites containing hazardous materials may be of interest for the additional impact that could be created by release of hazardous or toxic materials near a population centre, or for the economic impact an attack on a key site may have.

Effects of VBIED's

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

What you can do

If you think your site 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 your site

• Consider using physical barriers to keep all but authorised vehicles at a safe distance. Seek the advice of your police Counter Terrorism Security Adviser (CTSA) either through your local police service or through the NaCTSO website www.nactso.gov.uk 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 site 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 site blast resistant, paying particular attention to windows. Additionally you may consider additional protection around the storage areas for hazardous materials to ensure unauthorised vehicles are kept at a safe distance. Have the site reviewed by a qualified security engineer when seeking advice on protected spaces, communications, announcement systems and protected areas

• Establish 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.

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 safety regulations.

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

[Back to 'Contents']

fifteen chemical, biological and radiological (CBR) attacks

Since the early 1990s, concern that terrorists might use CBR materials as weapons has steadily increased. Terrorists may also seek to disperse such material stored or used on your site through conventional or improvised explosives. A significant concern is that terrorists may seek to unlawfully obtain such materials from your site for use in a CBR attack elsewhere. The hazards are:

Chemical

Poisoning or injury caused by chemical substances, including ex-military chemical warfare agents or legitimate but harmful (e.g. toxic) 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 materials 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 so far 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

• Check your air-handling systems and filters and replace or upgrade 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 police Counter Terrorism Security Adviser (CTSA) either through your local police service or through the NaCTSO website www.nactso.gov.uk.

• Secure holdings of toxic chemicals to prevent misuse

•If you have a designated protected space this may also be suitable as a CBR shelter, but seek specialist advice from your 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.

[Back to 'Contents']

sixteen suicide attacks

Suicide bombers may use a lorry, plane or other kind of vehicle as a bomb or may conceal explosives on their person. These 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 anyone or anything that has not been thoroughly searched. Ensure that no one visits your protected areas without your being sure of his or her identity or without proper authority. Seek further advice through your police Counter Terrorism Security Adviser (CTSA) either through your local police service or through the NaCTSO website www.nactso.gov.uk.
- 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 60

[Back to 'Contents']

seventeen firearm & weapon attacks

Attacks involving firearms and weapons are still infrequent but it is important to be prepared to cope with such an incident. The important advice below will help you plan.

In the event of an attack take these four actions:

Stay Safe

- Under immediate GUN FIRE – Take cover initially, but leave the area as soon as possible if safe to do so
- Nearby GUN FIRE - Leave the area immediately, if possible and it is safe to do so.
- Leave your belongings behind.
- Do not congregate at evacuation points.

COVER FROM GUN FIRE	COVER FROM VIEW
Substantial brickwork or concrete	Internal partition walls
Engine blocks of motor vehicles	Car doors
Base of large live trees	Wooden fences
Earth banks/hills/mounds	Curtains

REMEMBER - out of sight does not necessarily mean out of danger, especially if you are not in 'cover from gun fire.'

IF YOU CAN'T ESCAPE - consider locking yourself and others in a room or cupboard. Barricade the door then stay away from it.

If possible choose a room where escape or further movement is possible. Silence any sources of noise, such as mobile phones, that may give away your presence.

See

The more information that you can pass to police the better but NEVER risk your own safety or that of others to gain it. Consider using CCTV and other remote methods where possible to reduce the risk. If it is safe to do so, think about the following:

- Is it a firearms / weapons incident?
- What else are they carrying?
- Moving in any particular direction?
- Exact location of the incident.
- Number and description of gunmen.
- Type of firearm -long-barrelled or handgun.

• Are they communicating with others? • Number of casualties / people in the area.

Tell

• **POLICE** - contact them immediately by dialling 999 or via your control room, giving them the information shown under 'See' above.

• Use all the **channels of communication** available to you to inform staff, visitors, neighbouring premises, etc. of the danger.

Act

• Secure your immediate environment and other vulnerable areas.

• Keep people out of public areas, such as corridors and foyers.

• Move away from the door and remain quiet until told otherwise by appropriate authorities or if you need to move for safety reasons, such as a building fire.

Armed Police

In the event of an attack involving firearms or weapons, a Police Officer's priority is to protect and save lives. Please remember:

• Initially they may not be able to distinguish you from the gunmen.

• Officers may be armed and may point guns at you.

• They may have to treat the public firmly. Follow their instructions; keep hands in the air / in view.

• Avoid quick movement towards the officers and pointing, screaming or shouting.

Plan

Consider the following when planning for a firearms / weapons incident

1. How you would communicate with staff, visitors, neighbouring premises, etc.
2. What key messages would you give to them in order to keep them safe?
3. Have the ability to secure key parts of the building to hinder free movement of the gunmen.
3. Think about incorporating this into your emergency planning and briefings
4. Test your plan at least annually.

If you require further information then please liaise with your police Counter Terrorism Security Adviser (CTSA) either through your local police service or through the NaCTSO website www.nactso.gov.uk.

[Back to 'Contents']

eighteen 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.

Security Managers 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 intranet to communicate crime prevention and counter terrorism initiatives.

All sites should have a supply of posters and material (even via web links) to support crime prevention and counter terrorism messages and initiatives. Material supporting such initiatives including 'Know Your Customer' campaigns can be obtained from the local Counter Terrorist Security Adviser (CTSA) or from the NaCTSO web-site www.nactso.gov.uk .

All Security Managers should involve their local police CTSA when considering improvements to the site and / or its environs.

See Good Practice Checklist – Communication in Appendix 'I'

[Back to 'Contents']

nineteen 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.

Sites holding, storing, or otherwise using hazardous or dangerous materials are included in this operational definition.

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

Primary Purpose 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 (this list is not exhaustive):

- Significant interest being taken in the outside of the site including parking areas – delivery gates – doors – entrances
- Groups or individuals taking significant interest in the location of CCTV cameras and controlled areas including hazardous chemical stores.
- People using pictures – videoing - making notes – sketching of the security measures at sites. 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 or 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 time 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 the same 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 to ensure this is not happening.

• The same individual using 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 and in-depth questions of employees or others more familiar with the environment

• **Sightings of suspicious activity should be passed immediately to security management for CCTV monitoring and the event recorded for evidential purposes.**

Reconnaissance operatives may also seek additional information on:

• 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 CONFIDENTIAL ANTI-TERRORIST HOTLINE – 0800 789 321

ANY INCIDENT THAT REQUIRES AN IMMEDIATE RESPONSE – DIAL 999.

[Back to 'Contents']

twenty threat levels

Information about the national threat level is available on the Security Service, Home Office, and UK Intelligence Community websites. These addresses are in the 'Useful Contacts' section at the back of this booklet.

Terrorism threat levels are designed to give a broad indication of the likelihood of a terrorist attack. They are based on the assessment of a range of factors including current intelligence, recent events and what is known about terrorist intentions and capabilities. This information may well be incomplete and decisions about the appropriate security response should be made with this in mind.

In particular, those who own, operate, manage or work in hazardous sites are reminded that SUBSTANTIAL and SEVERE both indicate a high level of threat and that an attack might well come without warning.

Threat Level Definitions

CRITICAL	**AN ATTACK IS EXPECTED IMMINENTLY**
SEVERE	**AN ATTACK IS HIGHLY LIKELY**
SUBSTANTIAL	**AN ATTACK IS A STRONG POSSIBILITY**
MODERATE	**AN ATTACK IS POSSIBLE BUT NOT LIKELY**
LOW	**AN ATTACK IS UNLIKELY**

Response Levels

Response levels provide a broad indication of the protective security measures that should be applied at any particular time. They are informed by the threat level but also take into account specific assessments of vulnerability and risk.

Response levels tend to relate to sites, whereas threat levels usually relate to broad areas of activity. There are a variety of site specific security measures that can be applied within response levels, although the same measures will not be found at every location.

The security measures deployed at different response levels should not be made public, to avoid informing terrorists about what we know and what we are doing about it.

There are three levels of response which broadly equate to threat levels as shown below:

CRITICAL	**EXCEPTIONAL**
SEVERE	**HEIGHTENED**
SUBSTANTIAL	
MODERATE	**NORMAL**
LOW	

Response Level Definitions

RESPONSE LEVEL	DESCRIPTION
EXCEPTIONAL	Maximum protective security measures to meet specific threats and to minimise vulnerability and risk
HEIGHTENED	Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk.
NORMAL	Routine baseline protective security measures appropriate to your business and location.

What can I do now?

• Carry out a risk and vulnerability assessment that is specific to your site.

• Identify a range of practical protective security measures appropriate for each of the response levels. Your police Counter Terrorism Security Adviser (CTSA) can assist with this and can be contacted either through your local police service or through the NaCTSO website www.nactso.gov.uk.

• Make use of the good practice checklists on the following pages to assist you in your decision making process.

The counter measures to be implemented at each response level are a matter for individual premises or organisations and will differ according to a range of circumstances.

All protective security measures should be identified in advance of any change in threat and response levels and should be clearly notified to those staff responsible for ensuring compliance.

[Back to 'Contents']

good practice checklists

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

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

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

- What is relevant to your site?
- 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

Business Continuity

	YES	NO	UNSURE
Do you have a Business Continuity Plan?			
Do you regularly review and update your plan?			
Have you considered firearm and weapon attacks in your plans?			
Are your staff trained in activating and operating your plan?			
Have you prepared an emergency 'Grab Bag?			
Do you have access to an alternative workspace to use in an emergency?			
Are your critical documents adequately protected?			
Do you have copies of your critical records at a separate location?			
Do you have contingency plans in place to cater for the loss/ failure of key equipment?			

[Back to 'Contents']

appendix b

Housekeeping Good Practice

	YES	NO	UNSURE
Have you reviewed the use and location of all waste receptacles in and around your site?			
Do you keep external areas, entrances, exits, stairs, 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,			
Do you have copies of your critical records at a separate location?			
Do you have contingency plans in place to cater for the loss/ failure of key equipment?			

[Back to 'Contents']

appendix C

Access Control for Hazardous Sites

	YES	NO	UNSURE
Do you prevent all vehicles from entering goods or service areas until they are authorised by your security?			
Do you have in place physical barriers to keep all but authorised vehicles at a safe distance and to mitigate against a hostile vehicle attack?			
Is there clear demarcation identifying the public and private areas of your site?			
Do your staff, including contractors, cleaners and other employees wear ID badges at all times when on the site?			
Do you adopt a 'challenge culture' to anybody not wearing a pass in your private areas?			
Do you insist that details of contract vehicles and the identity of the driver and any passengers requiring permission to park and work in your site are authorised in advance?			
Do you require driver and vehicle details of contractor or delivery/collection vehicles in advance?			
Do all business visitors to your management and administration areas have to report to a reception area before entry and are they required to sign in and be issued with a visitors pass?			
Are business visitors' badges designed to look different from staff badges?			
Are all business visitors' badges collected from visitors when they leave the premises?			
Does a member of staff accompany business visitors at all times while in the private areas of your site?			
Is access to hazardous/toxic materials and chemicals adequately controlled?			

[Back to 'Contents']

appendix d

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 site?			
Have you considered the introduction of ANPR to complement your access control procedures?			
Do you have CCTV cameras covering critical areas in your business, such as hazardous material storage areas server rooms, and back up generators?			
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 complement the CCTV system during daytime and darkness hours?			
Do you regularly check the quality of your recordings?			
Are your 'contracted in' CCTV operators licensed by the Security Industry Authority (SIA)?			
Have you implemented operating procedures, codes of practice and audit trails?			
Is each CCTV camera doing what it was installed to do?			

[Back to 'Contents']

appendix e

Searching

	YES	NO	UNSURE
Do you exercise your search plan regularly?			
Do you carry out a systematic and thorough search of your site sector-by-sector as a part of a response to a general threat and in response to a specific incident?			
Does your search plan have a written checklist - signed by the searching officer as complete for the information of the Security Manager?			
Does your search plan include outside areas as well as internal parts of the venue?			
Have you considered a vehicle search regime at goods/service entrances that is flexible and can be tailored to a change in threat or response level?			
Do you conduct random overt searches of vehicles as a visual deterrent?			
Do sub-contractors and other service providers operating within the centre have their own search procedure with notification to management when complete?			
Have you considered a visitor search regime that is flexible and can be tailored to a change in threat or response level?			
Do you make use of your website/publications to inform contractors and visitors of your searching policies as well as crime prevention and counter terrorism messages?			
Do you have a policy to refuse entry to any vehicle whose driver refuses a search request?			
Are your searching staff trained and properly briefed on their powers and what they are searching for?			
Are staff trained to deal effectively with unidentified packages found within the site?			
Do you have sufficient staff to search effectively?			
Do you search your evacuation routes and assembly areas before they are used?			

[Back to 'Contents']

appendix f

Evacuation / 'Invacuation'

	YES	NO	UNSURE
Is evacuation part of your security plan?			
Is 'invacuation' into a protected space part of your security plan?			
Have you sought advice from a structural engineer to identify protected spaces within your building?			
Do you have nominated evacuation / 'invacuation' marshals?			
Does your evacuation plan include 'incident' assembly areas distinct from fire assembly areas?			
Have you determined evacuation routes?			
Have you agreed your evacuation / 'invacuation' plans with the police, emergency services and your neighbours?			
Do you have reliable, tested communications facilities in the event of an incident?			
Have persons with special needs been individually briefed?			
Do you have a review process for updating plans as required?			

[Back to 'Contents']

appendix g

Personnel Security

	YES	NO	UNSURE
During recruitment **you should** 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 signature			
Cheque book and bank card – with three statements and proof of signature			
Proof of residence – council tax, gas, electric, water or telephone bill			
EEA Nationals:			
Full EEA passport			
National Identity Card			
Other Nationals:			
Full Passport and A Home Office document confirming the individual's UK Immigration status and permission to work in UK			

[Back to 'Contents']

appendix h

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 longer required?			
Do you back up business critical information regularly?			
Do you have a securely contained back up at a different location from where you operate your business? (Fall back procedure)			
Have you invested in secure cabinets for your IT equipment?			
Have you implemented IT security advice provided by an authority such as CPNI e.g. 'Twenty Critical Controls' - www.cpni.gov.uk/advice/cyber/Critical-controls/ or the Department for Business, Innovation and Skills (BIS) - www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know			

[Back to 'Contents']

appendix i

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 Adviser (CTSA) and do you involve them in any site security developments?			
Do you speak with neighbours to your site on issues of security and crime that might affect you all?			
Do you remind your staff to be vigilant when traveling to and from work, and to report anything suspicious to the relevant authorities or police?			
Do you make use of your website, to communicate crime and counter terrorism initiatives?			

[Back to 'Contents']

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 'Unsure' to.

If you answered 'Unsure' to a question, find out more about that particular issue to reassure yourself that this 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 needs 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 http://www.cpni.gov.uk/security-planning/business-continuity-plan/bomb-threats/ to download a PDF and print it out.

Actions to be taken on receipt of a bomb threat:

Switch on tape recorder/voicemail (if connected)

Tell the caller which town/district you are answering from

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 premises manager of 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 premises manager 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?

Accent? If so, what type?_____

Rapid?

Deep?

Hoarse?

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 system?

Booth?

Music?

Factory machinery?

Office machinery?

Other? (specify) _____

OTHER REMARKS

_____

_____

_____

_____

Signature

_____

Date _____

Print name

[Back to 'Contents']

useful publications

Publications

Protecting Against Terrorism (3rd Edition)

This 52 page booklet gives 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 http://www.cpni.gov.uk/documents/publications/2010/2010002-protecting_against_terrorism_3rd_edition.pdf?epslanguage=en-gb or email: **enquiries@cpni.gsi.gov.uk** to request a copy.

Personnel Security

A number of booklets concerning personnel security have been developed by the CPNI and are available in PDF format. These provide a useful reference for security managers and human resource managers who are developing or reviewing their approach to personnel security. The booklets can be downloaded from http://www.cpni.gov.uk/advice/Personnel-security1/

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-sized 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 prevent, manage and recover from a range of threats to their business.

Both booklets and a viewable version of the 'Secure in the Knowledge' DVD are now available to download and view from the NaCTSO website www.nactso.gov.uk

[Back to 'Contents']

useful contacts

NaCTSO (National Counter Terrorism Security Office)

t. 020 7931 7142

www.nactso.gov.uk

MPS Counter Terrorism Security Coordination Unit (Seccos)

t. 020 7231 8589

email: SecCoRequests@met.police.uk

ACPO (Association of Chief Police Officers)

t. 020 7227 3434

www.acpo.police.uk/

Police Scotland

t. 0141 435 1230

www.scotland.police.uk/

Confidential Anti-terrorism Hotline

t. 0800 789321

Home Office

t. 020 7035 4848

https://www.gov.uk/government/topics/national-security

CAST (Centre for Applied Science and Technology) formerly HOSDB (Home Office Scientific Development Branch)

t. 01727 816400

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/115681/intro-to-cast.pdf

Department for Business, Innovation and Skills (BIS)

www.gov.uk/government/organisations/department-for-business-innovation-skills

Department for Energy and Climate Change (DECC)

www.gov.uk/government/organisations/department-of-energy-climate-change

Department for Transport (DfT)

Dangerous Goods Security Enquiries:

t: 020 7944 2881

e-mail: DGSecurity@dft.gsi.gov.uk

https://www.gov.uk/government/policies/providing-effective-regulation-of-freight-transport

CPNI (Centre for the Protection of National Infrastructure)

www.cpni.gov.uk

The Business Continuity Institute

t. 0870 603 8783

www.thebci.org

London Prepared

www.londonprepared.gov.uk

SIA (Security Industry Authority)

t. 020 7227 3600

www.sia.homeoffice.gov.uk

Chief Fire Officers Association

t. 01827 302300

www.cfoa.org.uk

Scottish Fire and Rescue Service

Scottish Fire and Rescue Service Headquarters
5 Whitefriars Crescent
Perth
PH2 0PA

Phone: 01738 475260 (Office hours are from 9am to 5pm, Monday to Friday)

http://www.firescotland.gov.uk/

National Risk Register

t. 020 7276 1234

www.gov.uk/government/organisations/cabinet-office

Cross-Sector Safety and Security Communications (CSSC)

www.vocal.co.uk/cssc/

Chemical Business Association Ltd
Lyme Building
Westmere Drive
Crewe
Cheshire
CW1 6ZD

t. 01270 258200
f. 0270 258444
e-mail: cba@chemical.org.uk
www.chemical.org.uk

Chemical Industries Association

www.cia.org.uk

[Back to 'Contents']

notes